Produkthandbuch

McAfee® Host Intrusion Prevention

Version 6.1

McAfee®
Systemschutz

Führende Intrusionspräventions-Lösungen

McAfee®

Produkthandbuch

McAfee® Host Intrusion Prevention

Version 6.1

McAfee®
Systemschutz

Führende Intrusionspräventions-Lösungen

McAfee®

COPYRIGHT

Copyright (c) 2007 McAfee, Inc. Alle Rechte vorbehalten.

Kein Teil dieser Veröffentlichung darf ohne schriftliche Erlaubnis von McAfee, Inc., ihren Lieferanten oder zugehörigen Tochtergesellschaften in irgendeiner Form oder mit irgendwelchen Mitteln vervielfältigt, übertragen, transkribiert, in einem Informationsabrufsystem gespeichert oder in eine andere Sprache übersetzt werden.

HINWEISE AUF MARKEN

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (UND IN KATAKANA), ACTIVESHIELD, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, EPOLICY ORCHESTRATOR, FIRST AID, FOUNDSTONE, GROUPSHIELD, GROUPSHIELD (UND IN KATAKANA), INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, MCAFEE, MCAFEE (UND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NET TOOLS, NET TOOLS (UND IN KATAKANA), NETSCAN, NETSHIELD, NUTS & BOLTS, OIL CHANGE, PRIMESUPPORT, SPAMKILLER, THREATSCAN, TOTAL VIRUS DEFENSE, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (UND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (UND IN KATAKANA) sind registrierte Marken oder eingetragene Marken von McAfee, Inc., bzw. der angeschlossenen Tochterunternehmen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Kennzeichen der McAfee-Markenprodukte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind Eigentum ihrer jeweiligen Besitzer.

LIZENZINFORMATIONEN

Lizenzvereinbarung

HINWEIS AN ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DER BESTELL-UNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, ALS DATEI AUF DER PRODUKT-CD ODER ALS DATEI VON DER WEBSITE, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE NICHT ALLEN BEDINGUNGEN DIESER VEREINBARUNG ZUSTIMMEN, INSTALLIEREN SIE DIE SOFTWARE NICHT. IN DIESEM FALL KÖNNEN SIE DAS PRODUKT GEGEN RÜCKERSTATTUNG DES KAUFPREISES AN MCAFEE ODER AN DIE STELLE ZURÜCKGEBEN, VON DER SIE ES ERWORBEN HABEN.

Hinweise

Dieses Produkt enthält oder enthält möglicherweise:

• Software, die vom OpenSSL-Projekt für die Verwendung im OpenSSL-Toolkit (http://www.openssl.org/) entwickelt wurde. • Kryptographiesoftware, die von Eric Young geschrieben wurde, und Software, die von Tim J. Hudson geschrieben wurde. • Einige Softwareprogramme, für die dem Endbenutzer eine Lizenz (oder Sublizenz) unter der GNU General Public License (GPL) oder anderen ähnlichen Freeware-Lizenzen erteilt wurde, die es dem Benutzer unter anderem erlauben, bestimmte Programme oder Teile solcher Programme zu kopieren, zu modifizieren und weiterzugeben sowie auf den Quellcode zuzugreifen. Bei Software, die GPL unterliegt und in ausführbarem Binärformat an andere Personen weitergegeben wird, muss diesen Benutzern auch der Quellcode zur Verfügung gestellt werden. Für alle Softwareprogramme, die durch die GPL abgedeckt sind, wird der Quellcode auf dieser CD verfügbar gemacht. Wenn Lizenzen für freie Software es erforderlich machen, dass McAfee Rechte zur Nutzung, Kopie oder Abänderung eines Softwareprogramms bereitstellt, die über die in diesem Vertrag eingeräumten Rechte hinausgehen, so haben diese Rechte Vorrang vor den Rechten und Einschränkungen aus diesem Vertrag. • Software, die ursprünglich von Henry Spencer geschrieben wurde, Copyright 1992, 1993, 1994, 1997 Henry Spencer. • Ursprünglich von Robert Nordier entwickelte Software, Copyright © 1996–7 Robert Nordier. • Von Douglas W. Sauder entwickelte Software. • Von Apache Software Foundation entwickelte Software (http://www.apache.org/). Eine Kopie des Lizenzvertrages dieser Software befindet sich unter www.apache.org/licenses/LICENSE-2.0.txt. • International Components for Unicode („ICU"), Copyright © 1995–2002 International Business Machines Corporation und andere. • Von CrystalClear Software, Inc., entwickelte Software, Copyright © 2000 CrystalClear Software, Inc. • FEAD® Optimizer®-Technologie, Copyright Netopsystems AG, Berlin, Deutschland. • Outside In® Viewer Technology © 1992–2001 Stellent Chicago, Inc., und/oder Outside In® HTML Export, © 2001 Stellent Chicago, Inc. • Software, die von Thai Open Source Software Center Ltd. und Clark Cooper urheberrechtlich geschützt ist, © 1998, 1999, 2000. • Software, die von Expat Maintainers urheberrechtlich geschützt ist. • Software, die von The Regents of the University of California urheberrechtlich geschützt ist, © 1996, 1989, 1998–2000. • Software, die von Gunnar Ritter urheberrechtlich geschützt ist. • Software, die von Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., urheberrechtlich geschützt ist, © 2003. • Software, die von Gisle Aas urheberrechtlich geschützt ist. © 1995–2003. • Software, die von Michael A. Chase urheberrechtlich geschützt ist, © 1999-2000. • Software, die von Neil Winton urheberrechtlich geschützt ist, © 1995–1996. • Software, die von RSA Data Security, Inc., urheberrechtlich geschützt ist, © 1990–1992. • Software, die von Sean M. Burke urheberrechtlich geschützt ist, © 1999, 2000. • Software, die von Martijn Koster urheberrechtlich geschützt ist, © 1995. • Software, die von Brad Appleton urheberrechtlich geschützt ist, © 1996–1999. • Software, die von Michael G. Schwern urheberrechtlich geschützt ist, © 2001. • Software, die von Graham Barr urheberrechtlich geschützt ist, © 1998. • Software, die von Larry Wall und Clark Cooper urheberrechtlich geschützt ist, © 1998–2000. • Software, die von Frodo Looijaard urheberrechtlich geschützt ist, © 1997. • Software, die von Python Software Foundation urheberrechtlich geschützt ist, Copyright © 2001, 2002, 2003. Eine Kopie des Lizenzvertrags dieser Software findet sich unter www.python.org. • Software, die von Beman Dawes urheberrechtlich geschützt ist, © 1994–1999, 2002. • Software, die von Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek geschrieben wurde, © 1997–2000 University of Notre Dame. • Software, die von Simone Bordet & Marco Cravero urheberrechtlich geschützt ist, © 2002. • Software, die von Stephen Purcell urheberrechtlich geschützt ist, © 2001. • Software, die von Indiana University Extreme! Lab (http://www.extreme.indiana.edu/) entwickelt wurde. • Software, die von International Business Machines Corporation und anderen urheberrechtlich geschützt ist, © 1995–2003. • Von der University of California, Berkeley, und deren Mitarbeitern entwickelte Software. • Software, die von Ralf S. Engelschall <rse@engelschall.com> zur Verwendung im mod_ssl-Projekt (http:// www.modssl.org/) entwickelt wurde. • Software, die von Kevlin Henney urheberrechtlich geschützt ist, © 2000–2002. • Software, die von Peter Dimov und Multi Media Ltd. urheberrechtlich geschützt ist, © 2001, 2002. • Software, die von David Abrahams urheberrechtlich geschützt ist, © 2001, 2002. Die Dokumentation befindet sich unter http://www.boost.org/libs/bind/bind.html. • Software, die von Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock urheberrechtlich geschützt ist, © 2000. • Software, die von Boost.org urheberrechtlich geschützt ist, © 1999–2002. • Software, die von Sean Nicolai M. Josuttis urheberrechtlich geschützt ist, © 1999. • Software, die von Jeremy Siek urheberrechtlich geschützt ist, © 1999–2001. • Software, die von Daryle Walker urheberrechtlich geschützt ist, © 2001. • Software, die von Chuck Allison und Jeremy Siek urheberrechtlich geschützt ist, © 2001, 2002. • Software, die von Samuel Krempp urheberrechtlich geschützt ist, © 2001. Aktualisierungen, Dokumentation und die Versionshistorie finden Sie unter http://www.boost.org. • Software, die von Doug Gregor urheberrechtlich geschützt ist (gregod@cs.rpi.edu), © 2001, 2002. • Software, die urheberrechtlich geschützt ist von Cadenza New Zealand Ltd., © 2000. • Software, die urheberrechtlich geschützt ist von Jens Maurer, © 2000, 2001. • Software, die urheberrechtlich geschützt ist von Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. • Software, die urheberrechtlich geschützt ist von Ronald Garcia, © 2002. • Software, die urheberrechtlich geschützt ist von David Abrahams, Jeremy Siek und Daryle Walker, © 1999–2001. • Software, die urheberrechtlich geschützt ist von Stephen Cleary (shammah@voyager.net), © 2000. • Software, die urheberrechtlich geschützt ist von Housemarque Oy <http://www.housemarque.com>, © 2001. • Software, die urheberrechtlich geschützt ist von Paul Moore, © 1999. • Software, die urheberrechtlich geschützt ist von Dr. John Maddock, © 1998–2002. • Software, die urheberrechtlich geschützt ist von Greg Colvin und Beman Dawes, © 1998, 1999. • Software, die urheberrechtlich geschützt ist von Peter Dimov, © 2001, 2002. • Software, die urheberrechtlich geschützt ist von Jeremy Siek und John R. Bandela, © 2001. • Software, die urheberrechtlich geschützt ist von Joerg Walter und Mathias Koch, © 2000–2002. • Software, die urheberrechtlich geschützt ist von Carnegie Mellon University, © 1989, 1991, 1992. • Software, die urheberrechtlich geschützt ist von Cambridge Broadband Ltd., © 2001–2003. • Software, die urheberrechtlich geschützt ist von Sparta, Inc., © 2003–2004. • Software, die urheberrechtlich geschützt ist von Cisco, Inc., und Information Network Center der Beijing University of Posts and Telecommunications, © 2004. • Software, die urheberrechtlich geschützt ist von Simon Josefsson, © 2003. • Software, die urheberrechtlich geschützt ist von Thomas Jacob, © 2003–2004. • Software, die urheberrechtlich geschützt ist von Advanced Software Engineering Limited, © 2004. • Software, die urheberrechtlich geschützt ist von Todd C. Miller, © 1998. • Software, die urheberrechtlich geschützt ist von The Regents of the University of California, © 1990, 1993, mit Code, der abgeleitet ist von Software, die Berkeley von Chris Torek erhalten hat.

PATENTINFORMATIONEN

Geschützt durch US-Patente 6.301.699; 6.412.071; 6.496.875; 6.668.289; 6.823.460.

Herausgegeben Februar 2007 / Host Intrusion Prevention-Software Version 6.1

DBN-100-DE

Inhalt

1 Einführung von Host Intrusion Prevention 9

Neue Funktionen dieser Version 10
Änderungen im Vergleich zur vorhergehenden Version 10
Neue Funktionen 10
Verwenden dieses Handbuchs 11
Lesergruppe 11
Konventionen 12
Produktinformationen 13
Standarddokumentation 13
Kontaktinformationen 14

2 Grundlegende Konzepte 15

IPS-Funktion 15
Signaturregeln 16
Verhaltensregeln 16
Ereignisse 16
Reaktionen 16
Ausnahmeregeln 17
Firewall-Funktion 17
Firewall-Regeln 17
Client-Firewall-Regeln 18
Anwendungsblockierfunktion 18
Blockierregeln für die Client-Anwendung 19
Allgemeine Funktion 19
Richtlinienverwaltung 19
Erzwingen von Richtlinien 19
Richtlinien und Richtlinienkategorien 20
Vererbung und Zuweisung von Richtlinien 21
Richtlinieneigentümerschaft 21
Sperren der Richtlinienzuweisung 21
Bereitstellung und Verwaltung 22
Vordefinierter Schutz 22
Adaptiver und Lernmodus 23
Feineinstellung 23
Berichte 24

3 Verwenden von ePolicy Orchestrator 25

Mit der Host Intrusion Prevention verwendete ePolicy Orchestrator-Vorgänge 26
ePolicy Orchestrator-Konsole 26
Richtlinienverwaltung 27
Eigentümer zu Richtlinien zuweisen 28
Generieren von Benachrichtigungen 29
Generieren von Berichten 29
Host Intrusion Prevention-Vorgänge 29
Installation des Host Intrusion Prevention-Servers 29
Bereitstellen der Host Intrusion Prevention-Clients 30
Anzeigen und Verwenden von Client-Daten 30
Clients in den adaptiven oder in den Lernmodus versetzen 31
Konfigurieren von Richtlinien 32
Feineinstellung 33
Verwenden der Hilfe 34

4 IPS-Richtlinien 36

Übersicht . . . 36
- Host- und Netzwerk-IPS-Signaturregeln . . . 37
- Vordefinierte IPS-Richtlinien . . . 38
- Direktzugriff . . . 39

Konfigurieren der Richtlinie für IPS-Optionen . . . 39
Konfigurieren der Richtlinie für den IPS-Schutz . . . 41
Konfigurieren der Richtlinie für IPS-Regeln . . . 44
Details der IPS-Regelrichtlinien . . . 45
- Ausnahmeregeln . . . 45
- Signaturen . . . 48
- Anwendungsschutzregeln . . . 56

IPS-Ereignisse . . . 60
- Anzeigen von Ereignissen . . . 61
- Konfigurieren der Ereignisansicht . . . 62
- Filtern von Ereignissen . . . 62
- Markieren von Ereignissen . . . 63
- Ähnliche Ereignisse markieren . . . 64
- Anzeigen von Ereignisdetails . . . 65
- Ereignisbasierte Ausnahmen und vertrauenswürdige Anwendungen erstellen . . . 66

IPS-Client-Regeln . . . 68
- Standard-Ansicht . . . 68
- Aggregierte Ansicht . . . 69

IPS-Ausnahmeregeln suchen . . . 70

5 Firewall-Richtlinien 72

Übersicht . . . 73
- HIP 6.0-Regeln . . . 73
- HIP 6.1-Regeln . . . 74
- Funktionsweise von Firewall-Regeln . . . 75
- Funktionsweise der statusbehafteten Filterung . . . 76
- Funktionsweise der statusbehafteten Paketinspizierung . . . 77
- Firewall-Regelgruppen und Verbindungsgruppen . . . 79
- Firewall – Lernmodus und adaptiver Modus . . . 81
- Quarantäne-Richtlinien und -Regeln . . . 82
- Migration von benutzerdefinierten 6.0-Firewall-Regeln zu 6.1-Regeln . . . 83
- Vordefinierte Firewall-Richtlinien . . . 84
- Direktzugriff . . . 84

Konfigurieren der Richtlinie für Firewall-Optionen . . . 85
Konfigurieren der Richtlinie für Firewall-Regeln . . . 87
- Erstellen neuer Richtlinien für Firewall-Regeln . . . 87
- Anzeigen und Bearbeiten von Firewall-Regeln . . . 90
- Erstellen einer neuen Firewall-Regel oder Firewall-Gruppe . . . 91
- Löschen einer Firewall-Regel oder -Gruppe . . . 94
- Anzeigen von Firewall-Client-Regeln . . . 94

Konfigurieren der Richtlinie für Quarantäneoptionen . . . 96
Konfigurieren der Richtlinie „Quarantäneregeln“ . . . 97
- Erstellen neuer Richtlinien für Quarantäneregeln . . . 97
- Anzeigen und Bearbeiten von Quarantäneregeln . . . 99
- Erstellen einer neuen Quarantäneregel oder -gruppe . . . 99
- Löschen einer Quarantäneregel oder -gruppe . . . 100

6 Anwendungsblockierrichtlinien 101

Übersicht . . . 101
- Anwendungserstellung . . . 101
- Anwendungs-Hooks . . . 102
- Vordefinierte Anwendungsblockierungsrichtlinien . . . 102
- Direktzugriff . . . 102

Konfigurieren der Richtlinie für die Anwendungsblockieroptionen 103
Konfigurieren der Richtlinie „Anwendungsblockierregeln“ 105
Erstellen neuer Richtlinien für Anwendungsblockierregeln 105
Anzeigen und Bearbeiten von Anwendungsblockierregeln 106
Erstellen neuer Anwendungsblockierregeln. 107
Löschen einer Anwendungsblockierregel. 108
Anzeigen von Client-Anwendungsregeln 109

7 Allgemeine Richtlinien 111

Übersicht 111
Vordefinierte Richtlinien „Allgemein“. 112
Konfigurieren von „Richtlinien erzwingen“ 113
Konfigurieren der Richtlinie „Client-UI“ 113
Erstellen und Anwenden einer Client-UI-Richtlinie 114
Konfigurieren der Richtlinie „Vertrauenswürdige Netzwerke“ 118
Konfigurieren der Richtlinie „Vertrauenswürdige Anwendungen“ 120
Erstellen und Anwenden der Richtlinie „Vertrauenswürdige Anwendungen“ 120
Erstellen vertrauenswürdiger Anwendungen 121
Vertrauenswürdige Anwendungen bearbeiten 123
Vertrauenswürdige Anwendungen aktivieren oder deaktivieren 123
Vertrauenswürdige Anwendungen löschen 123

8 Wartung 124

Feineinstellung einer Bereitstellung 124
Analysieren von IPS-Ereignissen. 124
Erstellen von Ausnahmeregeln und Regeln für vertrauenswürdige Anwendungen 125
Mit Client-Ausnahmeregeln arbeiten 125
Erstellen und Anwenden neuer Richtlinien 125
Richtlinienverwaltung und Tasks 126
Registerkarte „Richtlinien“. 126
Richtlinienkatalog 128
Ausführen von Server-Tasks. 131
Verzeichnis-Gateway. 131
Ereignisarchivierung. 131
Eigenschaftenübersetzung. 131
Einrichten von Benachrichtigungen für Ereignisse. 132
So funktionieren Benachrichtigungen. 132
Host Intrusion Prevention-Benachrichtigungen 133
Ausführen von Berichten 134
Vordefinierte Berichte. 134
Host Intrusion Prevention-Berichte 135
Aktualisieren von 139
Einchecken des Update-Pakets 139
Aktualisieren der Clients 140

9 Host Intrusion Prevention-Client 142

Windows-Client. 142
Symbol in Systemablage. 143
Client-Konsole. 144
Warnungen 147
Registerkarte „IPS-Richtlinie“ 153
Firewall-Richtlinie, Registerkarte 155
Anwendungsrichtlinie, Registerkarte 157
Registerkarte „Blockierte Hosts“ 159
Registerkarte „Anwendungsschutz“ 161
Registerkarte „Aktivitätsprotokoll“ 162
Solaris-Client 164
Richtlinienerzwingung mit dem Solaris-Client. 164
Problembehandlung. 164

Linux-Client 167
Richtlinienerzwingung mit dem Linux-Client 167
Anmerkungen zum Linux-Client 168
Fehlerbehebung 168

10 Häufig gestellte Fragen (FAQ) 172

A Schreiben von benutzerdefinierten Signaturen 177

Regelstruktur 177
Obligatorische allgemeine Abschnitte 178
Optionale allgemeine Abschnitte 180
Abschnittswertvariablen. 181
Benutzerdefinierte Windows-Signaturen 184
Klassendateien 184
Klasse „Isapi“ 187
Klasse „Registry“ 191
Klasse „Services“ 193
Benutzerdefinierte Solaris-Signaturen 196
Klasse UNIX_file 196
Erweiterte Details 198
Klasse UNIX_apache. 198
Benutzerdefinierte Linux-Signaturen. 200
Klasse UNIX_file 200
Zusammenfassung der Parameter und Richtlinien 201
Liste der Parameter entsprechend dem Typ. 201
Liste der Richtlinien entsprechend dem Typ. 201

Glossar 202

Index 212

1 Einführung von Host Intrusion Prevention

McAfee® Host Intrusion Prevention ist ein hostbasiertes Erkennungs- und Präventionssystem, das Systemressourcen und Anwendungen sowohl vor externen als auch vor internen Angriffen schützt.

Host Intrusion Prevention schützt vor dem unberechtigten Anzeigen, Kopieren, Ändern oder Löschen von Daten und einer Gefährdung von System- und Netzwerkressourcen und Anwendungen, die Daten speichern und ausgeben. Dies wird erreicht durch eine innovative Kombination aus Host-Intrusionspräventions-Systemsignaturen (HIPS), Netzwerk-Intrusionspräventions-Systemsignaturen (NIPS), Verhaltensregeln und Firewall-Regeln.

Host Intrusion Prevention ist vollständig integriert in ePolicy Orchestrator und verwendet ePolicy Orchestrator Framework zur Übertragung und Durchsetzung von Richtlinien. Die Teilung der Funktionen von Host Intrusion Prevention in IPS, Firewall, Anwendungsblockierung und allgemeine Funktionen bietet eine stärkere Kontrolle über die Bereitstellung von Richtlinienschutz und Schutzebenen für die Benutzer.

Der Schutz ist eingerichtet, sobald Host Intrusion Prevention installiert ist. Die Einstellungen für den Standardschutz erfordern so gut wie keine Feinabstimmung und ermöglichen eine schnelle Bereitstellung auf breiter Ebene. Wenn Sie einen umfassenderen Schutz wünschen, können Sie Richtlinien bearbeiten und hinzufügen, um die Feinabstimmung einer Bereitstellung vorzunehmen.

Grundlegende Informationen über die Verwendung dieses Produkts und dieses Handbuchs finden Sie unter:

- *Neue Funktionen dieser Version*
- *Verwenden dieses Handbuchs*
- *Produktinformationen*
- *Kontaktinformationen*

Neue Funktionen dieser Version

Host Intrusion Prevention 6.1 kann vollständig in ePolicy Orchestrator 3.6.1 integriert werden, um die Client-Anwendung auf den Windows-, Solaris- und Linux-Plattformen zu verwalten. Der ePolicy Orchestrator-Agent ist erforderlich und seine Version hängt von der Plattform ab, auf der der Client installiert ist. Für Windows ist der ePO-Agent 3.5.5 oder höher erforderlich. Für Solaris und Linux ist der ePO-Agent 3.7 erforderlich.

Änderungen im Vergleich zur vorhergehenden Version

- Zwei Firewall-Richtlinienkategorien, die statusbehaftete Firewall-Funktionalität für 6.1 Windows-Clients zusätzlich zu statischer Firewall-Funktionalität für 6.0.X-Clients bieten.
  - Richtlinien für **Firewall-Regeln** und **Quarantäneregeln** sind statusbehaftete Firewall-Regelrichtlinien, die nur Host Intrusion Prevention 6.1-Clients verwalten.
  - 6.0-Richtlinien für **Firewall-Regeln** und **Quarantäneregeln** sind veraltete statische Firewall-Regelrichtlinien, die Host Intrusion Prevention 6.0.X-Clients verwalten.
- Statusbehaftete Firewall-Optionen in der **Firewall-Optionen**-Richtlinie zur Aktivierung der **FTP-Protokollprüfung** und Festlegung von **TCP-Verbindungstimeout** und **Virtuellem UDP-Verbindungstimeout**.
- Die Verbindungen berücksichtigenden Gruppen in der **Firewall-Regel**-Richtlinie wurden verbessert.
  - Ein DNS-Suffix wurde als Kriterium für Netzwerkzugriff hinzugefügt.
  - Es wird zwischen verkabelten und kabellosen Netzwerkverbindungen unterschieden.

Neue Funktionen

- Unterstützung für Linux-Clients auf Red Hat Enterprise 4 mit SE Linux.
  - Verwaltung von IPS-Richtlinien durch die ePO-Konsole.
  - Anwendung für adaptiven Modus.
- Unterstützung für Solaris-Clients auf Solaris 8, 9 und 10, 32-Bit- und 64-Bit-Kernels.
  - Verwaltung von IPS-Richtlinien durch die ePO-Konsole.
  - Anwendung für adaptiven Modus.
  - Schutz von Webservern, einschließlich Sun One und Apache.
  - Fähigkeit zum Upgrade von Entercept 5.1 für Solaris.

Verwenden dieses Handbuchs

Dieses Handbuch enthält die folgenden Informationen über die Konfiguration und Verwendung Ihres Produkts. Informationen über Systemvoraussetzungen und Installationsanweisungen finden Sie im *Konfigurationshandbuch*.

- *Einführung von Host Intrusion Prevention*
  Eine Übersicht über das Produkt, einschließlich einer Beschreibung neuer oder geänderter Funktionen, eine Übersicht über dieses Handbuch; McAfee-Kontaktinformationen.
- *Grundlegende Konzepte*
  Eine Erklärung der Grundelemente von Host Intrusion Prevention und ihre Funktionsweise.
- *Verwenden von ePolicy Orchestrator*
  Eine Erläuterung der Verwendung von Host Intrusion Prevention und ePolicy Orchestrator.
- *IPS-Richtlinien*
  Eine Erläuterung des Einsatzes der IPS-Richtlinien.
- *Firewall-Richtlinien*
  Eine Erläuterung des Einsatzes der Firewall-Richtlinien.
- *Anwendungsblockierrichtlinien*
  Eine Erläuterung des Einsatzes von Richtlinien, die Anwendungen blockieren.
- *Allgemeine Richtlinien*
  Eine Erläuterung des Einsatzes von allgemeinen Richtlinien.
- *Wartung*
  Eine Erläuterung der Wartung von Host Intrusion Prevention.
- *Host Intrusion Prevention-Client*
  Eine Erläuterung des Einsatzes des Client.
- *Häufig gestellte Fragen (FAQ)*
  Antworten auf häufig gestellte Fragen über Host Intrusion Prevention.
- *Schreiben von benutzerdefinierten Signaturen*
  Anhang über das Schreiben von Kundensignaturen.
- *Glossar*
- *Index*

Lesergruppe

Diese Informationen wenden sich an Netzwerk- oder IT-Administratoren, die für das Host-Intrusionserkennungs- und -präventionssystem Ihres Unternehmens verantwortlich sind.

Konventionen

In diesem Handbuch gelten die folgenden Konventionen:

Schmalfett	Alle Wörter auf der Benutzeroberfläche, z. B. Optionen, Menüs, Schaltflächen und Dialogfenster. **Beispiel:** Geben Sie den Namen des **Benutzers** und das **Kennwort** des gewünschten Kontos an.

`Courier`	Der Pfad eines Ordners oder Programms; Text, der vom Benutzer wie vorgegeben eingegeben wird (z. B. ein Befehl an der Systemaufforderung).
	Beispiel:
	Der Standard-Speicherort für dieses Programm lautet:
	`C:\Programme\McAfee\EPO\3.5.0`
	Führen Sie diesen Befehl auf dem Client-Computer aus:
	`C:\SETUP.EXE`

Kursiv	Steht für eine Betonung oder die Einführung eines neuen Begriffs; für die Bezeichnungen der Produktdokumentation und für Themen (Überschriften) innerhalb des Materials. **Beispiel:** Weitere Informationen finden Sie im *VirusScan Enterprise Produkthandbuch*.
Blau	Eine Webadresse (URL) und/oder ein Live-Link. Besuchen Sie die McAfee-Website unter: http://www.mcafee.com
<BEGRIFF>	Generische Begriffe werden in spitze Klammern gesetzt. **Beispiel:** Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf <SERVER>.
	Hinweis: Zusätzliche Informationen, wie eine Alternativmethode für die Ausführung desselben Befehls.
	Tipp: Vorschläge für empfohlene Vorgehensweisen und Tipps von McAfee für die Prävention von Gefahren, Leistung und Effizienz.
	Achtung: Wichtige Empfehlungen zum Schutz Ihres Computersystems, des Unternehmens, der Software-Installation oder der Daten.
	Warnung: Wichtiger Hinweis, um einen Benutzer beim Umgang mit der Hardware vor Verletzungen zu schützen.

Produktinformationen

Sofern nicht anders angegeben, handelt es sich bei der Produktdokumentation um Dateien im PDF-Format von Adobe Acrobat (Version 6.0). Sie befinden sich auf der Produkt-CD oder können von der entsprechenden McAfee-Site heruntergeladen werden.

Standarddokumentation

Installationshandbuch: Verfahrensweisen für die Bereitstellung und die Verwaltung von unterstützten Produkten mithilfe der Verwaltungssoftware ePolicy Orchestrator.

Produkthandbuch: Produkteinführung und Funktionsbeschreibung, detaillierte Anweisungen zum Konfigurieren der Software, Informationen zur Bereitstellung, sich wiederholende Aufgaben und Verfahrensabläufe.

Hilfe: Wertvolle und genaue Informationen, die über die Schaltfläche **Hilfe** der Software-Anwendung abgerufen werden können.

Schnellreferenzkarte: Eine handliche Karte mit Informationen über grundlegende Produktfunktionen, häufig durchgeführte Routineaufgaben und gelegentlich durchgeführte kritische Aufgaben. *Die Karte liegt der Produkt-CD bei.*

Versionshinweise: *ReadMe*. Produktinformationen, gelöste und bekannte Probleme und Ergänzungen kurz vor Drucklegung oder Änderungen an Produkt oder Dokumentation. (Eine Textdatei ist Teil der Software-Anwendung und befindet sich auf der Produkt-CD.)

Kontaktinformationen

Threat Center: McAfee Avert® Labs http://www.mcafee.com/us/threat_center/default.asp

Avert Labs – Bedrohungsbibliothek
http://vil.nai.com

Avert Labs WebImmune & Beispiel an Avert senden *(Anmeldedaten erforderlich)*
https://www.webimmune.net/default.asp

Avert Labs DAT Benachrichtigungsdienst
http://vil.nai.com/vil/signup_DAT_notification.aspx

Download-Website http://www.mcafee.com/us/downloads/

Produkt-Upgrades *(Gültige Gewährungsnummer erforderlich)*

Sicherheits-Updates (DAT-Dateien, Engine)

HotFix- und Patch-Versionen

- **Für Sicherheitsschwachstellen** *(Öffentlich verfügbar)*
- **Für Produkte** *(ServicePortal-Konto und gültige Gewährungsnummer erforderlich)*

Produktbewertung

McAfee Beta-Programm

Technischer Support http://www.mcafee.com/us/support/

KnowledgeBase-Suche
http://knowledge.mcafee.com/

McAfee Technischer Support ServicePortal *(Anmeldedaten erforderlich)*
https://mysupport.mcafee.com/eservice_enu/start.swe

Kundendienst

Web
http://www.mcafee.com/us/support/index.html
http://www.mcafee.com/us/about/contact/index.html

Telefon – USA, Kanada und Lateinamerika (gebührenfrei):
+1-888-VIRUS NO oder **+1-888-847-8766** Montag bis Freitag, 8:00 bis 20:00 Uhr, Central Time

Professionelle Dienste

Unternehmen: http://www.mcafee.com/us/enterprise/services/index.html

Kleine und mittlere Unternehmen: http://www.mcafee.com/us/smb/services/index.html

2 Grundlegende Konzepte

McAfee® Host Intrusion Prevention ist ein hostbasiertes Intrusionsschutzsystem. Es schützt vor bekannten und unbekannten Angriffen, einschließlich Würmern, Trojanischen Pferden, Pufferüberlauf, kritischen Änderungen von Systemdateien und Berechtigungseskalationen. Die Host Intrusion Prevention-Verwaltung wird über die ePolicy Orchestrator-Konsole zur Verfügung gestellt. Sie ermöglicht das Festlegen und Anwenden von Host Intrusion Prevention, Firewall, Anwendungsblockierung und allgemeinen Richtlinien. Host Intrusion Prevention-Clients werden auf Servern und Desktops bereitgestellt und funktionieren als unabhängige Schutzeinheiten. Sie melden ihre Aktivitäten an ePolicy Orchestrator und erhalten Aktualisierungen für neue Angriffsdefinitionen.

In diesem Abschnitt werden vier Funktionen von Host Intrusion Prevention sowie die Zusammenarbeit mit ePolicy Orchestrator beschrieben. Er behandelt außerdem die folgenden Themen:

- *IPS-Funktion*
- *Firewall-Funktion*
- *Anwendungsblockierfunktion*
- *Allgemeine Funktion*
- *Richtlinienverwaltung*
- *Bereitstellung und Verwaltung*

IPS-Funktion

Die IPS (Intrusion Prevention System)-Funktion überwacht alle System- und API-Aufrufe und blockiert solche, die Schäden anrichten könnten. Host Intrusion Prevention bestimmt, welcher Prozess einen Aufruf verwendet, den Sicherheitskontext, in dem der Prozess ausgeführt wird, und die Ressource, auf die zugegriffen wird. Ein Treiber auf Kernel-Ebene, der umgeleitete Einträge in der Systemaufruftabelle im Benutzermodus erhält, überwacht die Systemaufrufkette. Wenn Aufrufe gemacht werden, vergleicht der Treiber die Aufrufanforderung mit einer Datenbank, die kombinierte Signaturen und Verhaltensregeln enthält, um zu bestimmen, ob eine Aktion erlaubt, blockiert oder protokolliert werden soll.

Signaturregeln

Signaturregeln sind Muster von Zeichen, die mit einem Datenstrom abgeglichen werden können. Beispielsweise kann eine Signaturregel nach einer bestimmten Zeichenfolge in einer HTTP-Anforderung suchen. Wenn die Zeichenfolge mit einer Zeichenfolge eines bekannten Angriffs übereinstimmt, werden bestimmte Maßnahmen getroffen. Diese Regeln bieten Schutz gegen bekannte Angriffe.

Signaturen werden für bestimmte Anwendungen und bestimmte Betriebssysteme entworfen, beispielsweise Webserver, wie Apache, IIS und NES/iPlanet. Die meisten Signaturen schützen das gesamte Betriebssystem. Manche schützen dagegen bestimmte Anwendungen.

Verhaltensregeln

Hart kodierte Verhaltensregeln definieren ein Profil mit legitimer Aktivität. Aktivitäten, die nicht mit dem Profil übereinstimmen, werden als verdächtig angesehen, und es wird eine Reaktion ausgelöst. Beispielsweise kann eine Verhaltensregel besagen, dass nur ein Webserver-Vorgang auf HTML-Dateien zugreifen kann. Wenn ein anderer Vorgang auf eine HTML-Datei zugreift, werden entsprechende Maßnahmen ergriffen. Diese Regeln bieten einen Schutz vor Zero-Day-Angriffen (Angriffe auf neue, bisher unbekannte Sicherheitslücken) und Pufferüberläufen.

Ereignisse

IPS-Ereignisse werden generiert, wenn ein Client eine Verletzung einer Signatur oder einer Verhaltensregel erkennt. Ereignisse werden auf der Registerkarte „IPS-Ereignisse“ unter „IPS-Regeln“ protokolliert. Administratoren können diese Ereignisse überwachen, um Verstöße gegen die Systemregeln anzuzeigen und zu analysieren. Sie können dann die Reaktionen auf Ereignisse anpassen oder Regeln für Ausnahmen oder vertrauenswürdige Anwendungen erstellen, um die Anzahl an Ereignissen zu senken und die Feineinstellung für die Schutzeinstellungen vorzunehmen.

Reaktionen

Eine Reaktion ist die Antwort eines Client, wenn er eine Signatur eines bestimmten Schweregrads erkennt.

Ein Client reagiert auf eine der drei folgenden Arten:

- **Ignorieren** – Keine Reaktion; das Ereignis wird nicht protokolliert und der Vorgang wird nicht verhindert.
- **Protokollieren** – Das Ereignis wird protokolliert, aber der Vorgang wird nicht verhindert.
- **Verhindern** – Das Ereignis wird protokolliert und der Vorgang wird verhindert.

Eine Sicherheitsrichtlinie kann z. B. Folgendes besagen: Wenn ein Client eine Signatur der Ebene **Informationen** erkennt, protokolliert er das Vorkommen dieser Signatur und überlässt die Verarbeitung des Vorgangs dem Betriebssystem. Wenn er dagegen eine Signatur der Ebene **Hoch** erkennt, verhindern er den Vorgang.

Die Protokollierung kann direkt für jede Signatur aktiviert werden.

Ausnahmeregeln

Eine Ausnahme stellt eine Regel für das Überschreiben von blockierten Aktivitäten dar. In manchen Fällen kann das als Angriff definierte Verhalten Teil der normalen Arbeitsroutine eines Benutzers sein oder eine Aktivität, die legal ist für eine geschützte Anwendung. Um diese Signatur zu überschreiben, können Sie eine *Ausnahme* erstellen, die legitime Aktivitäten erlaubt. Eine Ausnahme kann z. B. besagen, dass für einen bestimmten Client ein Vorgang ignoriert wird.

Sie können diese Ausnahmen manuell erstellen oder Clients in den Adaptiven Modus versetzen und es ihnen erlauben, Client-Ausnahmeregeln zu erstellen. Um zu gewährleisten, dass einige Signaturen nie überschrieben werden, bearbeiten Sie die Signatur und deaktivieren Sie die Optionen **Client-Regeln zulassen**. Sie können die Client-Ausnahmen in der ePolicy Orchestrator-Konsole nachverfolgen und sie in einer regulären und einer aggregierten Ansicht anzeigen. Verwenden Sie diese Client-Regeln, um neue Richtlinien zu erstellen oder sie zu bestehenden Richtlinien hinzuzufügen, die Sie auf andere Clients anwenden können.

Firewall-Funktion

Die Firewall von Host Intrusion Prevention agiert als Filter zwischen einem Computer und dem Netzwerk oder Internet, mit dem er verbunden ist. Die Richtlinie für die 6.0 Firewall-Regeln verwendet die statische Paketfilterung, bei der zunächst allgemeine, dann spezielle Regeln geprüft werden. Wenn ein Paket analysiert wird und es mit einer Firewall-Regel übereinstimmt, wobei Kriterien wie die IP-Adresse, die Portnummer und der Pakettyp angewendet werden, wird das Paket erlaubt oder blockiert. Wenn keine übereinstimmende Regel gefunden wird, wird das Paket verweigert. Die aktuelle Version der Richtlinie für Firewall-Regeln verwendet die statusbehaftete Paketfilterung sowie die statusbehaftete Paketinspizierung.

Andere Funktionen:

- Ein Quarantänemodus, in den Client-Computer versetzt werden können; Sie können auf diesen Modus einen rigiden Satz von Firewall-Regeln anwenden, der festlegt, mit wem in Quarantäne genommene Clients kommunizieren können.
- Mit einer Verbindungsgruppe können Sie spezielle Richtliniengruppen erstellen, die auf einem bestimmten Verbindungstyp für jeden Netzwerkadapter basieren.

Firewall-Regeln

Sie können je nach Bedarf einfache oder komplexe Firewall-Regeln erstellen. Host Intrusion Prevention unterstützt Regeln, die basieren auf:

- Verbindungstyp (Netzwerk oder kabellos).
- IP- und Nicht-IP-Protokollen.
- Richtung des Netzwerkverkehrs (eingehend, ausgehend oder beides).
- Anwendungen, die den Datenverkehr verursacht haben.
- Dienst oder Port, der von einem Computer verwendet wird (als Empfänger oder Sender).

- Dienst oder Port, der von einem Remote-Computer verwendet wird (als Empfänger oder Sender).
- Quell- und Ziel-IP-Adressen.
- Tageszeit oder Woche, zu/in der das Paket gesendet oder empfangen wurde.

Client-Firewall-Regeln

Wie bei IPS-Regeln kann ein Client im adaptiven oder Lernmodus Client-Regeln erstellen, die eine blockierte Aktivität zulassen. Sie können die Client-Regeln zurückverfolgen und sie in der Standard- oder der aggregierten Ansicht anzeigen. Verwenden Sie diese Client-Regeln, um neue Richtlinien zu erstellen oder sie zu bestehenden Richtlinien hinzuzufügen, die auf andere Clients angewendet werden können.

Anwendungsblockierfunktion

Die Anwendungsblockierfunktion von Host Intrusion Prevention überwacht verwendete Anwendungen und lässt sie zu oder blockiert sie.

Host Intrusion Prevention ermöglicht zwei Arten der Anwendungsblockierung:

- Anwendungserstellung
- Anwendungs-Hooks

Wenn Host Intrusion Prevention die *Erstellung* von Anwendungen überwacht, sucht sie nach Anwendungen, deren Ausführung versucht wird. In den meisten Fällen gibt es keine Probleme. Es gibt jedoch einige Viren, die z. B. versuchen, Programme auszuführen, die für das System gefährlich sind. Sie können dies verhindern, indem Sie Anwendungsregeln erstellen, die Firewall-Regeln ähnlich sind und die nur die Ausführung von Programmen zulassen, die für einen Benutzer erlaubt sind.

Wenn Host Intrusion Prevention das *Hooking* von Anwendungen überwacht, sucht sie nach Programmen, die einen Versuch unternehmen, sich an andere Anwendungen zu binden („Hooking"). Manchmal ist dieses Verhalten harmlos, gelegentlich jedoch handelt es sich hierbei um ein verdächtiges Verhalten, das auf einen Virus oder einen anderen Angriff auf Ihr System hinweist.

Sie können Host Intrusion Prevention so konfigurieren, dass nur die Anwendungserstellung, das Anwendungs-Hooking oder beides überwacht wird.

Die Anwendungsblockierfunktion funktioniert wie die Firewall-Funktion. Erstellen Sie eine Liste von Anwendungsregeln – eine Regel für jede Anwendung, die Sie erlauben oder blockieren möchten. Immer, wenn Host Intrusion Prevention eine Anwendung entdeckt, die versucht, eine andere Anwendung zu starten oder sich an sie zu binden, wird die Anwendungsregelliste geprüft; mit deren Hilfe wird bestimmt, ob eine Anwendung erlaubt oder blockiert wird.

Blockierregeln für die Client-Anwendung

Clients im adaptiven oder Lernmodus können Client-Regeln erstellen, um das Erstellen oder Hooking von blockierten Anwendungen zu erlauben, die sowohl in der Standard- als auch in der aggregierten Ansicht angezeigt werden. Verwenden Sie diese Client-Regeln genau wie IPS- und Firewall-Client-Regeln, um neue Richtlinien zu erstellen oder sie zu bestehenden Richtlinien hinzuzufügen, die auf andere Clients angewendet werden können.

Allgemeine Funktion

Die Funktion „Allgemein“ von Host Intrusion Prevention ermöglicht den Zugriff auf Richtlinien, die allgemeiner Natur sind und nicht spezifisch für IPS-, Firewall- oder Anwendungsblockierfunktionen gelten. Dazu gehören:

- Aktivieren oder Deaktivieren der Erzwingung aller Richtlinien.
- Bestimmen, wie die Client-Schnittstelle angezeigt wird und ein Zugriff erfolgt.
- Erstellen und Bearbeiten vertrauenswürdiger Netzwerkadressen und Subnetze.
- Erstellen und Bearbeiten vertrauenswürdiger Anwendungen, um das Auslösen von falschen positiven Ereignissen zu verhindern.

Richtlinienverwaltung

Eine *Richtlinie* ist eine Sammlung von Host Intrusion Prevention-Einstellungen, die Sie über die ePolicy Orchestrator-Konsole konfigurieren und dann auf dem Host Intrusion Prevention-Client erzwingen. Durch Richtlinien können Sie gewährleisten, dass die Sicherheitssoftware auf verwalteten Systemen so konfiguriert ist, dass die Anforderungen an Ihre Umgebung erfüllt sind.

Über die ePolicy Orchestrator-Konsole können Sie die Host Intrusion Prevention-Richtlinien von einem zentralen Standort aus konfigurieren. Richtlinien sind Teil der NAP-Datei von Host Intrusion Prevention, die bei der Installation von Host Intrusion Prevention zum Master-Repository hinzugefügt wurden.

Erzwingen von Richtlinien

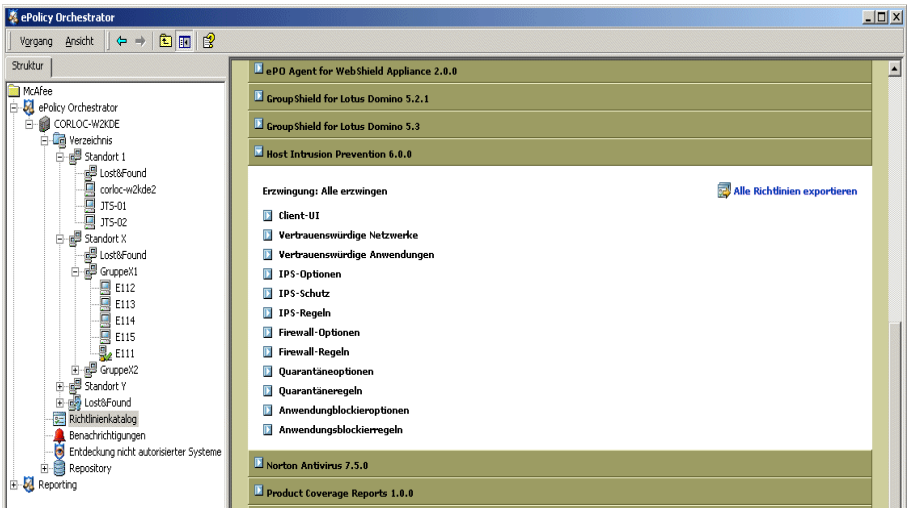
Wenn Sie Host Intrusion Prevention-Richtlinien über die ePolicy Orchestrator-Konsole ändern, werden die Änderungen auf den verwalteten Systemen beim nächsten Kommunikationsintervall zwischen Agent und Server (Agent-to-Server Communication Interval, ASCI) übernommen. Laut Standardeinstellung ist dieses Intervall auf 60 Minuten festgelegt.

Host Intrusion Prevention-Richtlinien können sofort erzwungen werden, indem Sie eine Reaktivierung von der ePolicy Orchestrator-Konsole aus senden.

Richtlinien und Richtlinienkategorien

Die Richtlinieninformationen für jedes Produkt werden in *Kategorien* eingeteilt. Jede Richtlinienkategorie bezieht sich auf eine bestimmte Untermenge von Richtlinien. Im **Richtlinienkatalog** wird jede Richtlinienkategorie eines Produkts angezeigt, wenn Sie den Produktnamen erweitern.

Abbildung 2-1 Richtlinienkatalog



Eine *benannte Richtlinie* ist ein konfigurierter Satz von Richtliniendefinitionen für eine bestimmte Richtlinienkategorie. Sie können beliebig viele benannte Richtlinien für jede Richtlinienkategorie erstellen, ändern oder löschen. Im **Richtlinienkatalog** werden benannte Richtlinien für eine bestimmte Kategorie angezeigt, wenn Sie den Namen der Kategorie erweitern.

Jede Richtlinienkategorie hat eine Richtlinie mit dem Namen **Globaler Standard**. Sie können diese Richtlinie nicht bearbeiten oder löschen.

Sie können mithilfe von zwei Host Intrusion Prevention-Richtlinienkategorien **IPS-Regeln** und **Regeln für vertrauenswürdige Anwendungen** mehr als eine benannte Richtlinieninstanz zuweisen. Außerdem bieten Ihnen diese Richtlinienkategorien ein Profil von IPS-Richtlinien und Richtlinien für vertrauenswürdige Anwendungen, die angewendet werden können.

Abbildung 2-2 Ein Profil mit zwei Richtlinieninstanzen für vertrauenswürdige Anwendungen

Vertrauenswürdige Anwendungen
Weitere Richtlinie zuweisen
Vertrauenswürdige Anwendungen sind in allen Umgebungen sicher, haben keine bekannten Schwachstellen und sind dazu berechtigt, alle Vorgänge auszuführen. Von diesen Vorgängen sind diejenigen ausgenommen, durch die die Anwendung einem Fremdeinfluss ausgesetzt ist. Verwenden Sie diesen Abschnitt, um bestimmte auf Client-Profilen basierende Richtlinien zu erstellen. Anschließend können Sie eine Kombination dieser Richtlinien zuweisen, um den richtigen Schutz auf den Clients zu konfigurieren.
Richtlinienname
Erstellt am
Geerbt von
Vererbt durch
Löschen
Sperren
Zeile bearbeiten
McAfee 1
Global Default
--
--
Bearbeiten
McAfee 2
(diesem Knoten)
--
--
Bearbeiten

Vererbung und Zuweisung von Richtlinien

Richtlinien werden auf beliebige Knoten in der Verzeichnisstruktur der Konsole entweder durch Vererbung oder Zuweisung angewendet. *Vererbung* bestimmt, ob die Richtlinieneinstellungen für einen beliebigen Knoten von dessen übergeordnetem Element übernommen werden sollen. Laut Standardeinstellung ist die Vererbung im gesamten Verzeichnis aktiviert. Sie können diese Vererbung durch direkte *Zuweisung* von Richtlinien durchbrechen. Da Host Intrusion Prevention durch ePolicy Orchestrator verwaltet wird, haben Sie die Möglichkeit, Richtlinien zu erstellen und diese unabhängig von der Vererbung zuzuweisen. Wenn Sie diese Vererbung durch Zuweisung einer neuen Richtlinie an einer beliebigen Position im Verzeichnis unterbrechen, erben alle untergeordneten Knoten diese neue Richtlinie.

Richtlinieneigentümerschaft

Während alle Richtlinien verfügbar sind, benötigt jede Richtlinie einen zugewiesenen Eigentümer. Laut Standardeinstellung ist der Eigentümer einer Richtlinie der globale oder der Site-Verwalter, der sie erstellt hat.

Die Eigentümerschaft gewährleistet, dass nur der globale Verwalter oder der Eigentümer der benannten Richtlinie diese Richtlinie ändern kann. Jeder Administrator kann alle Richtlinien im Katalog verwenden; ändern kann sie jedoch nur der Eigentümer oder der globale Administrator.

Wenn Sie eine Richtlinie, deren Eigentümer nicht Sie sind, zu Knoten des von Ihnen verwalteten Verzeichnisses zuweisen und der Eigentümer der Richtlinie diese ändert, gelten diese Änderungen für alle Systeme, denen diese Richtlinie zugewiesen wurde.

Wenn Sie eine Richtlinie verwenden und steuern möchten, die das Eigentum eines anderen Administrators ist, sollten Sie eine Kopie dieser Richtlinie anfertigen und dann das Duplikat dieser Richtlinie zuweisen.

Sperren der Richtlinienzuweisung

Ein globaler Verwalter kann die Zuweisung einer Richtlinie an jedem beliebigen Speicherort im Verzeichnis sperren. Durch das Sperren einer Richtlinienzuweisung wird der Wechsel der Zuweisung von einer Richtlinie durch eine andere von Seiten der Benutzer unterbunden. Die Vererbung erfolgt mit der Richtlinie.

Das Sperren von Richtlinienzuweisungen ist hilfreich, wenn ein globaler Verwalter eine bestimmte Richtlinie an der Spitze des Verzeichnisses konfiguriert und zuweist, um zu gewährleisten, dass kein anderer Benutzer sie durch eine andere benannte Richtlinie an einem beliebigen Speicherort des Verzeichnisses ersetzt.

Durch das Sperren von Richtlinien wird nicht verhindert, dass der Eigentümer Änderungen an den Einstellungen der benannten Richtlinie vornimmt. Achten Sie daher darauf, wenn Sie eine Richtlinienzuweisung sperren möchten, dass Sie der Eigentümer der Richtlinie sind.

Bereitstellung und Verwaltung

Die Bereitstellung und Verwaltung der Host Intrusion Prevention-Clients findet über ePolicy Orchestrator statt. In dieser ePO-Konsolenstruktur können Sie Clients hierarchisch nach Attributen gruppieren. Sie können z. B. eine erste Ebene für einen geografischen Standort und eine zweite Ebene für die Betriebssystemplattform oder die IP-Adresse festlegen. Wir empfehlen, dass Sie Clients in Gruppen – basierend auf Host Intrusion Prevention-Konfigurationskriterien – anordnen, einschließlich des Systemtyps (Server oder Desktop), der Verwendung von wichtigen Anwendungen (Web, Datenbank oder Mail-Server) und der strategischen Positionen (DMZ oder Internet). Sie können Clients, die ein gemeinsames *Verwendungsprofil* haben, in einer gemeinsame Gruppe in der Konsolenstruktur platzieren. Tatsächlich können Sie eine Gruppe nach diesem Verwendungsprofil benennen, z. B. *Webserver*.

Wenn Sie die Konsolenstruktur verwenden, in der die Rechner gemäß ihrem Typ, ihrer Funktion oder ihrem geografischen Standort gruppiert sind, können Sie Verwaltungsfunktionen für dieselben Kategorien ganz einfach trennen. Mit Host Intrusion Prevention können Sie außerdem die Verwaltungsaufgaben basierend auf den Produktfunktionen, wie IPS oder Firewall, trennen.

Mit dieser Version von Host Intrusion Prevention und ePolicy Orchestrator sind richtlinienunabhängige Einheiten, die über verschiedene Knoten freigegeben werden können. Sie weisen eine Richtlinie für jede Kategorie in einer Funktion von Host Intrusion Prevention zu. Bei manchen Kategorien, wie IPS-Regeln, sind mehrere Richtlinien erlaubt, wobei sie entweder von einem übergeordneten Knoten geerbt oder auf den Knoten selbst angewendet werden können. In diesem Fall übernimmt Host Intrusion Prevention die Behandlung von Konflikten, wobei die striktere Regel zuerst angewendet wird. Wenn Sie einem Gruppenknoten die entsprechenden Richtlinien zuweisen, erbt durch die Vererbung in ePolicy Orchestrator jedes System unterhalb dieses Knotens die Konfiguration des übergeordneten Elements.

Die Bereitstellung der Host Intrusion Prevention-Clients auf Tausenden von Computern ist einfach zu verwalten, da die meisten Clients in nur wenige Anwendungsprofile passen. Die Verwaltung einer großen Bereitstellung reduziert sich auf die Verwaltung einiger weniger Richtlinienregeln. Mit der Erweiterung der Bereitstellung sollten neu hinzugefügte Systeme in ein oder mehrere vorhandene Profile passen. Sie können dann einfach in dem richtigen Gruppenknoten in der Konsolenstruktur platziert werden.

Vordefinierter Schutz

Host Intrusion Prevention bietet einen grundlegenden Schutz durch die Standard-Richtlinieneinstellungen von McAfee. Für diesen „fertigen" Schutz ist keine Feinabstimmung erforderlich und er verursacht nur wenige Ereignisse. Clients können zunächst im großen Stil bereitgestellt werden, sogar noch bevor Sie die Bereitstellung fein einstellen. In vielen Umgebungen, in denen der Client auf Arbeitsstationen oder Laptops installiert ist, kann dieser Grundschutz ausreichend sein.

Ein erweiterter Schutz ist außerdem über einige vordefinierte IPS- und Firewall-Richtlinien verfügbar. Ein Profil für Server benötigt beispielsweise einen stärkeren Schutz als den grundlegenden Arbeitsstationsschutz. Sie können auch alternativ die vordefinierten erweiterten Schutzrichtlinien als Basis verwenden, um benutzerdefinierte Richtlinien zu erstellen.

Adaptiver und Lernmodus

Um die Schutzeinstellungen noch feiner abzustimmen, können Host Intrusion Prevention-Clients auf Client-Seite Ausnahmeregeln für Serverrichtlinien erstellen, die legitime Aktivitäten blockieren. Das Erstellen von Client-Regeln ist erlaubt, wenn Clients in den *adaptiven* oder *Lernmodus* versetzt werden. Im adaptiven Modus, der für IPS-, Firewall- und Anwendungsblockierfunktionen verfügbar ist, werden Client-Regeln erstellt, ohne dass der Benutzer eingreifen muss. Im Lernmodus, der für Firewall- und Anwendungsblockierfunktionen zur Verfügung steht, muss der Benutzer dem System sagen, ob eine Client-Regel erstellt werden soll oder nicht.

Bei beiden Modi werden Ereignisse bei den gefährlichsten Angriffen, wie Pufferüberläufen, analysiert. Wenn die Aktivität als normal und erforderlich für den Arbeitsablauf betrachtet wird, erstellen Host Intrusion Prevention-Clients Client-Regeln, um Vorgänge zu erlauben, die andernfalls blockiert würden. Indem Sie Clients in den adaptiven Modus oder in den Lernmodus versetzen, erhalten Sie für diese Agenten eine Tuningkonfiguration. Host Intrusion Prevention ermöglicht es Ihnen anschließend, beliebige, alle oder keine Client-Regeln anzuwenden und sie in servergesteuerte Richtlinien zu konvertieren. Der adaptive und der Lernmodus können jederzeit deaktiviert werden, um den Intrusionspräventions-Schutz des Systems zu erhöhen.

In großen Unternehmen hat das Vermeiden von Unterbrechungen der Geschäftsaktivitäten häufig Priorität über Sicherheitsbelange. Neue Anwendungen müssen z. B. regelmäßig auf einigen Client-Computern installiert werden und Sie haben möglicherweise keine Zeit oder keine Ressourcen, um umgehend eine Feinabstimmung vorzunehmen. Mit Host Intrusion Prevention können bestimmte Clients für den IPS-Schutz in den adaptiven Modus versetzt werden. Diese Computer stellen das Profil für eine neu installierte Anwendung und leiten die erstellten Client-Regeln an den Server weiter. Der Verwalter kann diese Client-Regeln auf vorhandene oder neue Richtlinien übertragen, die dann die Richtlinie auf andere Computer anwenden, um die neue Software zu verwalten.

Feineinstellung

Als Teil der Bereitstellung von Host Intrusion Prevention müssen Sie einige eindeutige *Verwendungsprofile* bezeichnen und für sie Richtlinien erstellen. Dies erreichen Sie am besten, wenn Sie eine Testbereitstellung einrichten und dann damit beginnen, die Zahl der falschen positiven und generierten Ereignisse zu verringern. Dieser Vorgang wird Feinabstimmung oder *Tuning* genannt.

Stärkere IPS-Regeln bieten beispielsweise mehr Signaturen, die eine breitere Palette von Verletzungen anvisieren und damit wesentlich mehr Ereignisse generieren als in einer Basisumgebung. Wenn Sie den erweiterten Schutz anwenden, empfehlen wir Ihnen die Verwendung der IPS-Schutzrichtlinie, um den Nutzen zu erhöhen. Dazu gehört die Zuordnung jeder Sicherheitsebene (Hoch, Mittel, Niedrig und Information) zu einer Reaktion (Verhindern, Protokollieren, Ignorieren). Indem anfangs alle Sicherheitsebenen mit Ausnahme von „Hoch“ auf „Ignorieren“ festgelegt werden, werden nur die Sicherheitssignaturen von „Hoch“ angewendet. Die anderen Ebenen können nach und nach beim Durchführen der Feinabstimmung erhöht werden.

Sie können die Zahl der falschen Positive verringern, indem Sie *Ausnahmeregeln*, *vertrauenswürdige Anwendungen* und *Firewall-Regeln* erstellen. Ausnahmeregeln sind Mechanismen für das Überschreiben einer Sicherheitsrichtlinie unter bestimmten Umständen. Vertrauenswürdige Anwendungen sind Anwendungsprozesse, die immer erlaubt sind. Firewall-Regeln bestimmen, ob Datenverkehr zulässig ist und ob die Paketübertragung erlaubt oder blockiert wird.

Berichte

Mit Berichten können Sie Daten über ein bestimmtes Element abrufen und sie nach einer bestimmten Untermenge von Daten filtern, z. B. Ereignisse der Ebene „Hoch“, die von bestimmten Clients für eine bestimmte Zeitspanne berichtet werden. Berichte können als E-Mail-Nachrichten geplant und gesendet werden.

3 Verwenden von ePolicy Orchestrator

Sie müssen ePolicy Orchestrator verwenden, um Host Intrusion Prevention zu konfigurieren und zu verwalten. Dazu sind die folgenden drei grundlegenden Tasks erforderlich:

- **Installieren/Checken Sie die Host Intrusion Prevention-Server-Dateien und das Client-Paket ein.**

  Checken Sie die Server-Dateien von Host Intrusion Prevention, die eine NAP-Datei umfassen, den Inhalt mit den Standardsignaturen und -regeln sowie die Berichte mit dem Host Intrusion Prevention-Installationsprogramm im ePolicy Orchestrator-Repository ein. Checken Sie das Client-Paket von Host Intrusion Prevention in das ePolicy Orchestrator-Repository ein. Einzelheiten finden Sie im *Host Intrusion Prevention 6.0-Installationshandbuch*.

- **Bereitstellen der Host Intrusion Prevention-Clients.**

  Verwenden Sie die ePolicy Orchestrator-Konsole, um die Host Intrusion Prevention-Clients auf den in der Konsolenstruktur unter Verzeichnis angezeigten Computern bereitzustellen. Einzelheiten finden Sie im *Produkthandbuch von ePolicy Orchestrator 3.6*.

- **Konfigurieren der Host Intrusion Prevention-Richtlinien.**

  Konfigurieren Sie die IPS-, Firewall-, Anwendungsblockier- sowie die allgemeinen Richtlinien, die Sie auf die Clients anwenden möchten. Die Standardeinstellungen der Richtlinien realisieren einen grundlegenden Schutz. Für einen verstärkten Schutz müssen Sie die Bereitstellung allerdings verfeinern und die Richtlinien an Ihre Umgebung anpassen. Einzelheiten finden Sie in den entsprechenden Kapiteln dieses Handbuchs.

- **Zuweisen von Eigentümern zu Richtlinien im Richtlinienkatalog.**

  Im Richtlinienkatalog werden die Eigentümer von Richtlinien festgelegt. Einzelheiten finden Sie im *Produkthandbuch von ePolicy Orchestrator 3.6*.

- **Richtlinienaktualisierungen der Host Intrusion Prevention an Clients senden.**

  ePolicy Orchestrator sendet Aktualisierungsinformationen an die Host Intrusion Prevention-Clients. Die Clients setzen die Richtlinien durch, sammeln Ereignisinformationen und übertragen diese Informationen zurück an ePolicy Orchestrator. Die Interaktion zwischen Client und Server wird durch die Einstellungen der ePolicy Orchestrator-Agentenrichtlinie festgelegt. Einzelheiten finden Sie im *Produkthandbuch von ePolicy Orchestrator 3.6*.

- **Einrichten von Benachrichtigungen in ePolicy Orchestrator für Host Intrusion Prevention-Ereignisse.**

  Einzelheiten finden Sie im *Produkthandbuch von ePolicy Orchestrator 3.6*.

- **Ausführen der Berichte in ePolicy Orchestrator, um die Ereignis- und Schutzergebnisse anzuzeigen.**

  Die Informationen über die Aktivität des Host Intrusion Prevention-Client werden an ePolicy Orchestrator gesendet und in dessen Datenbank gespeichert. Verwenden Sie die Konsole, um Berichte über den Host Intrusion Prevention-Schutz auszuführen.

Weitere Informationen zur Verwendung der Host Intrusion Prevention mit ePolicy Orchestrator finden Sie unter folgenden Themen:

- *Mit der Host Intrusion Prevention verwendete ePolicy Orchestrator-Vorgänge*
- *Host Intrusion Prevention-Vorgänge*

Mit der Host Intrusion Prevention verwendete ePolicy Orchestrator-Vorgänge

Einige grundlegende Funktionen, die von Host Intrusion Prevention verwendet werden, werden durch ePolicy Orchestrator-Funktionen ausgeführt. Einzelheiten zur Verwendung dieser Funktionen finden Sie in der ePolicy Orchestrator-Dokumentation. In diesem Dokument finden Sie eine kurze Übersicht über diese Funktionen sowie Einzelheiten zu den spezifischen Bereichen für Host Intrusion Prevention.

ePolicy Orchestrator-Konsole

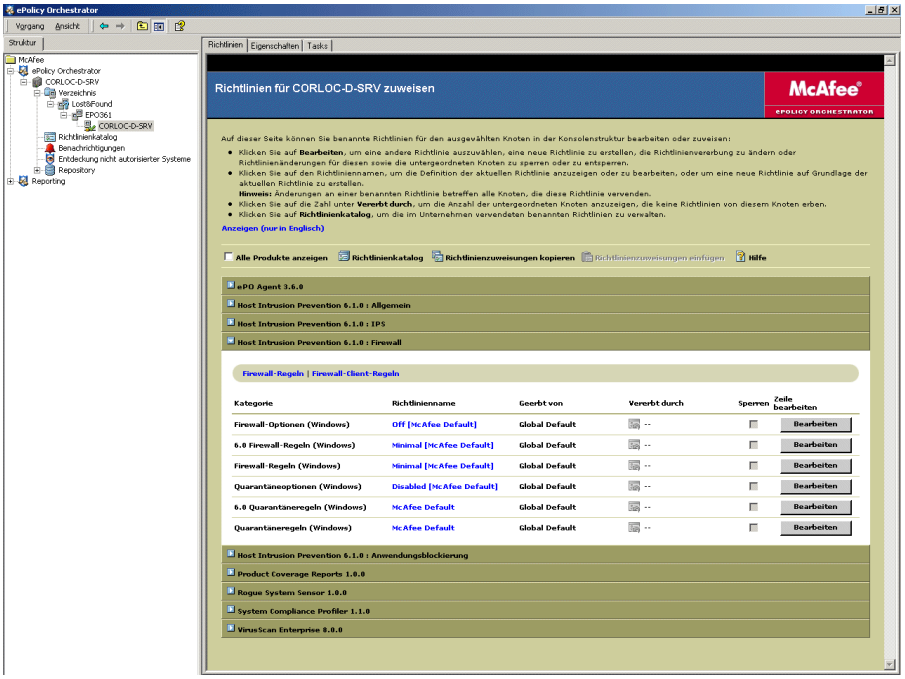
Verwenden Sie die ePolicy Orchestrator-Konsole, um Host Intrusion Prevention zu verwalten. Einzelheiten finden Sie im *Produkthandbuch von ePolicy Orchestrator 3.6*.

Die ePolicy Orchestrator-Konsole ist in zwei Hauptbereiche unterteilt: eine Konsolenstruktur und einen Detailbereich.

In der Konsolenstruktur wählen Sie unter **Verzeichnis** die ePolicy Orchestrator-Knoten aus (Computer, Gruppen und Sites), auf die Sie die Richtlinien der Host Intrusion Prevention anwenden. Diese Struktur enthält außerdem Links zu den anderen Hauptfunktionen der Konsolenoberfläche, einschließlich des Richtlinienkatalogs, der Benachrichtigungen und Berichte.

Im Detailbereich werden die Funktionseinstellungen der in der Konsolenstruktur ausgewählten Knoten angezeigt.

Abbildung 3-1 ePolicy Orchestrator-Konsole



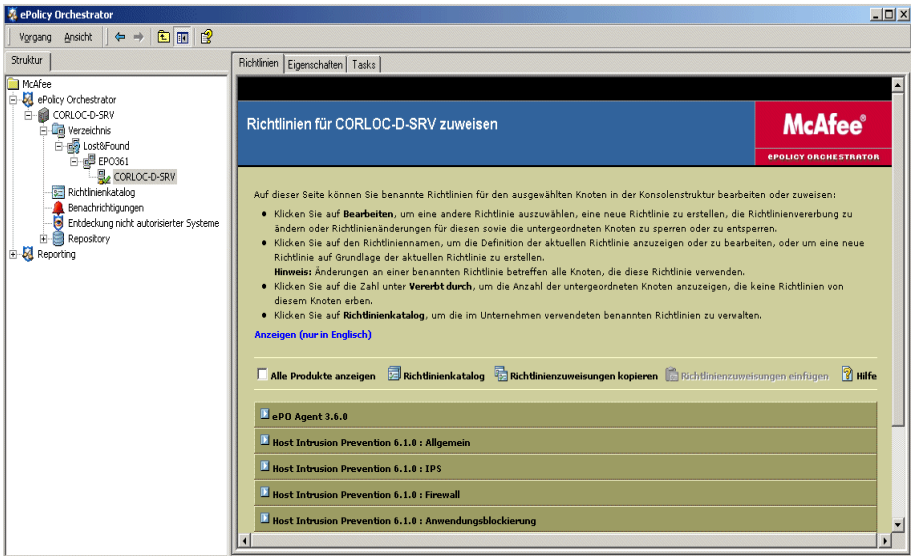
Richtlinienverwaltung

Eine Richtlinie ist eine Sammlung von Software-Einstellungen, die von Ihnen erstellt, konfiguriert und erzwungen werden. Sie können auf alle im Verzeichnis vorhandenen Knoten, für die Sie eine Berechtigung besitzen, Standardrichtlinien oder selbst erstellte benutzerdefinierte Richtlinien anwenden. Vor oder nach der Bereitstellung eines Produkts können Sie Richtlinien konfigurieren und zuweisen. Jede Richtlinienkategorie gibt an, ob die Richtlinie nur für einen Windows-Client **(Windows)** oder für alle Windows-, Solaris- und Linux-Clients **(Alle Plattformen)** gilt.

Sie können für beliebige Knoten des Verzeichnisses festlegen, ob alle oder keine der ausgewählten Richtlinien durchgesetzt werden sollen.

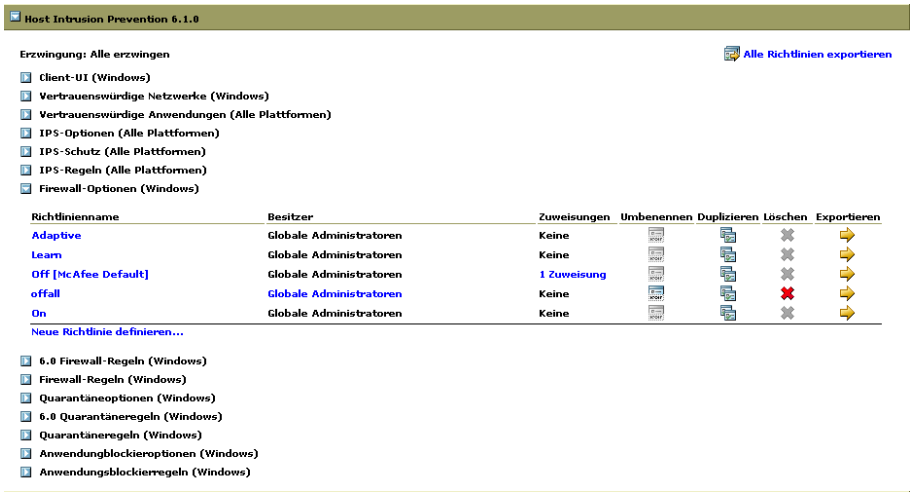
Auf der Seite **Richtlinien zuweisen**, die angezeigt wird, wenn Sie einen Knoten auswählen, können Sie entweder angeben, dass Richtlinien für Produkte oder für Produktfunktionen erzwungen werden sollen.

Abbildung 3-2 Seite „Richtlinien zuweisen“


ePolicy Orchestrator
Vorgang Ansicht
Struktur
McAfee
ePolicy Orchestrator
CORLOC-D-SRV
Verzeichnis
Lost&Found
EPO361
CORLOC-D-SRV
Richtlinienkatalog
Benachrichtigungen
Entdeckung nicht autorisierter Systeme
Repository
Reporting
Richtlinien Eigenschaften Tasks
Richtlinien für CORLOC-D-SRV zuweisen
McAfee
ePOLICY ORCHESTRATOR
Auf dieser Seite können Sie benannte Richtlinien für den ausgewählten Knoten in der Konsolenstruktur bearbeiten oder zuweisen:
Klicken Sie auf Bearbeiten, um eine andere Richtlinie auszuwählen, eine neue Richtlinie zu erstellen, die Richtlinienvererbung zu ändern oder Richtlinienänderungen für diesen sowie die untergeordneten Knoten zu sperren oder zu entsperren.
Klicken Sie auf den Richtliniennamen, um die Definition der aktuellen Richtlinie anzuzeigen oder zu bearbeiten, oder um eine neue Richtlinie auf Grundlage der aktuellen Richtlinie zu erstellen.
Hinweis: Änderungen an einer benannten Richtlinie betreffen alle Knoten, die diese Richtlinie verwenden.
Klicken Sie auf die Zahl unter Vererbt durch, um die Anzahl der untergeordneten Knoten anzuzeigen, die keine Richtlinien von diesem Knoten erben.
Klicken Sie auf Richtlinienkatalog, um die im Unternehmen verwendeten benannten Richtlinien zu verwalten.
Anzeigen (nur in Englisch)
Alle Produkte anzeigen
Richtlinienkatalog
Richtlinienzuweisungen kopieren
Richtlinienzuweisungen einfügen
Hilfe
ePO Agent 3.6.0
Host Intrusion Prevention 6.1.0 : Allgemein
Host Intrusion Prevention 6.1.0 : IPS
Host Intrusion Prevention 6.1.0 : Firewall
Host Intrusion Prevention 6.1.0 : Anwendungsblockierung

Auf der Seite **Richtlinienkatalog** können Sie Richtlinienzuweisungen und -eigentümer anzeigen.

Abbildung 3-3 Richtlinienkatalog



Eigentümer zu Richtlinien zuweisen

Sämtliche Richtlinien für Host Intrusion Prevention, für die Sie Berechtigungen besitzen, sind auf der Seite **Richtlinienkatalog** verfügbar. Damit kein Benutzer die Richtlinien eines anderen Benutzers ändern kann, wird jeder Richtlinie ein Eigentümer zugewiesen: der globale Administrator oder der Site-Administrator, der die Richtlinie erstellt hat.

Nur der Ersteller einer Richtlinie oder ein globaler Administrator kann eine Richtlinie ändern oder löschen. Alle Verwalter können sämtliche auf der Seite **Richtlinienkatalog** vorhandenen Richtlinien anwenden – aber lediglich der Eigentümer und der globale Verwalter können eine Richtlinie ändern.

Wenn Sie Segmenten des Verzeichnisses eine Richtlinie zuweisen, die sich nicht in Ihrem Besitz befindet, dann denken Sie daran, dass bei einer Änderung der Richtlinie durch den Eigentümer alle Knoten, denen diese Richtlinie zugewiesen ist, diese Änderungen empfangen. Wenn Sie eine Richtlinie verwenden möchten, die das Eigentum eines anderen Administrators ist, sollten Sie eine Kopie dieser Richtlinie anfertigen und dann das Duplikat diesem Knoten zuweisen.

Generieren von Benachrichtigungen

Durch E-Mail-, Pager- und SNMP-Trap-Benachrichtigungen können Sie sich über alle Ereignisse informieren lassen, die auf den Host Intrusion Prevention-Clients oder direkt auf dem Server auftreten. Sie können Regeln konfigurieren, über die beim Empfangen und Verarbeiten bestimmter Host Intrusion Prevention-Ereignisse auf dem ePolicy Orchestrator-Server Nachrichten oder SNMP-Traps gesendet oder externe Befehle ausgeführt werden. Mit dieser sehr gut konfigurierbaren Benachrichtigungsfunktion können Sie festlegen, welche Ereigniskategorien eine Benachrichtigung generieren und in welchen Zeitabständen diese gesendet werden.

Generieren von Berichten

Die auf den Client-Systemen arbeitenden Host Intrusion Prevention-Clients senden Informationen an den Server, der diese in einer Berichtsdatenbank speichert. Mithilfe dieser gespeicherten Informationen werden Berichte und Anforderungen ausgeführt. Es gibt acht vordefinierte Berichte, die in zwei Hauptkategorien unterteilt sind: IPS-Berichte und Firewall-Berichte. Weitere Informationen dazu finden Sie unter *Ausführen von Berichten* auf Seite 134.

Host Intrusion Prevention-Vorgänge

Im Folgenden finden Sie eine kurze Übersicht aller produktspezifischen Aspekte des Einsatzes von Host Intrusion Prevention. Einzelheiten zur Verwendung dieser Funktionen finden Sie in diesem Dokument.

Installation des Host Intrusion Prevention-Servers

Bevor Sie Clients bereitstellen können, müssen Sie den Management-Server installieren. Eine detaillierte Anleitung finden Sie im *Installationshandbuch von Host-Intrusion prevention*.

Bereitstellen der Host Intrusion Prevention-Clients

Clients bilden das Element der Host Intrusion Prevention-Bereitstellung, das den Schutz bietet. Idealerweise sollten alle in einer Arbeitsumgebung vorhandenen Systeme durch Client-Software geschützt sein. Es empfiehlt sich, die Bereitstellung in mehreren Phasen durchzuführen:

- **Legen Sie einen ersten Client-Einsatzplan fest.** Auch wenn Sie die Host Intrusion Prevention-Clients auf jedem Host (Server und Desktops) in Ihrem Unternehmen bereitstellen, empfehlen wir, dass Sie zunächst die Clients auf einer begrenzten Anzahl an repräsentativen Systemen installieren und ihre Konfiguration feinabstimmen. Nach dem Tunen der Bereitstellung können Sie weitere Clients bereitstellen und die in der ersten Phase erstellten Richtlinien, Ausnahmen und Client-Regeln nutzen.
- **Legen Sie für Ihre Clients eine Namenskonvention fest.** Clients werden in der Konsolenstruktur, in bestimmten Berichten und in den durch Aktivitäten im Client erzeugten Ereignisdaten durch Ihren Namen identifiziert. Clients können die Namen der Hosts annehmen, auf denen sie installiert sind. Sie können ihnen aber auch während der Installation spezifische Client-Namen zuweisen. Es empfiehlt sich, für**.**Clients eine Namenskonvention festzulegen, die von allen Benutzern, die mit der**.**Bereitstellung der Host Intrusion Prevention arbeiten, problemlos interpretiert werden kann.
- **Installieren der Clients.** Clients werden zusammen mit einem standardmäßigen Satz von IPS-, Firewall- und Anwendungsblockierrichtlinien sowie Richtlinien für allgemeine Regeln installiert. Neue Richtlinien mit aktualisierten Regeln können später vom Server übertragen werden.
- **Logische Gruppierung der Clients.** Clients können nach beliebigen Kriterien gruppiert werden. Die Gruppierung muss allerdings zur Hierarchie der Konsolenstruktur passen. Beispiel: Sie können Clients nach ihrem geografischen Standort, ihrer Funktion im Unternehmen oder nach den Systemmerkmalen gruppieren.

Eine detaillierte Anleitung finden Sie im *Host Intrusion Prevention-Installationshandbuch*.

Anzeigen und Verwenden von Client-Daten

Wenn Sie Ihre Clients installiert und gruppiert haben, ist die Bereitstellung abgeschlossen. Es sollten nun *Ereignisse* eintreten, die auf den Clients durch Aktivitäten ausgelöst werden, die die festgelegte IPS-Sicherheitsrichtlinie verletzen. Wenn Sie Clients in den adaptiven Modus versetzt haben, werden *Client-Regeln* erstellt, die angeben, welche Client-Ausnahmeregeln erstellt werden. Die Analyse dieser Daten hilft Ihnen beim Tunen der Bereitstellung.

Für die Analyse der Ereignisdaten zeigen Sie in der IPS-Funktion die Registerkarte **IPS-Ereignis** an. Sie können dort bis zu den Details eines Ereignisses gelangen – beispielsweise welcher Prozess ein Ereignis ausgelöst hat, wann das Ereignis erzeugt wurde und welcher Client es erzeugt hat. Analysieren Sie das Ereignis und ergreifen Sie die erforderlichen Aktionen, um die Bereitstellung der Host Intrusion Prevention feinabzustimmen und besser auf Angriffe reagieren zu können. Auf der Registerkarte **IPS-Ereignis** werden die standardmäßigen clientbasierten und netzwerkbasierten Intrusionspräventionssignaturen sowie benutzerdefinierte hostbasierte Signaturen angezeigt.

Um Client-Regeln zu analysieren, zeigen Sie die Registerkarte **Client-Regeln** an. Client-Regeln werden auch in den Firewall- und Anwendungsblockierfunktionen angezeigt. Dort sehen Sie, welche Regeln erstellt wurden. Sie können die Regeln aggregieren, um nach den verbreitetsten allgemeinen Regeln zu suchen. Und Sie können eine Regel direkt in eine Richtlinie verschieben, damit Sie für andere Clients angewendet wird.

Darüber hinaus bietet Ihnen die Berichtsfunktion detaillierte Berichte über Ereignisse, Client-Regeln und die Konfiguration von Host Intrusion Prevention. Mithilfe dieser Berichte können Sie andere Mitglieder Ihres Teams und Vorgesetzte über Aktivitäten in Ihrer Umgebung informieren.

Clients in den adaptiven oder in den Lernmodus versetzen

Ein wichtiges Element im Tuning-Prozess stellt das Versetzen der Host Intrusion Prevention-Clients in den adaptiven Modus für die IPS-, Firewall- und Anwendungsblockierung sowie das Versetzen in den Lernmodus für die Firewall- und Anwendungsblockierung dar. Über diese Modi können Clients Client-Ausnahmeregeln für Verwaltungsrichtlinien erstellen. Im adaptiven Modus geschieht dies automatisch, ohne Interaktion mit dem Benutzer. Im Lernmodus muss der Benutzer dem System bei einem Ereignis mitteilen, wie es sich verhalten soll.

In diesen Modi wird bei einem Ereignis zuerst geprüft, ob es sich um einen schwerwiegenden Angriff handelt, wie beispielsweise um einen Pufferüberlauf. Wenn die Aktivität als regulär und für das Unternehmen erforderlich eingestuft wird, werden Client-Ausnahmeregeln erstellt. Indem Sie repräsentative Clients in den adaptiven Modus oder in den Lernmodus versetzen, erhalten Sie für diese Agenten eine Tuningkonfiguration. Host Intrusion Prevention erlaubt Ihnen dann, beliebige, alle oder keine der Client-Regeln in Serverrichtlinien zu konvertieren. Wenn das Tunen abgeschlossen ist, können Sie den adaptiven Modus bzw. den Lernmodus deaktivieren, um die Intrusionsprävention des Systems zu verstärken.

- Führen Sie die Clients während mindestens einer Woche im adaptiven oder Lernmodus aus. Dieser Zeitraum ist notwendig, damit die Clients alle normalerweise auftretenden Aktivitäten erkennen. Versuchen Sie, die beiden Modi während geplanter Aktivitäten zu aktivieren – beispielsweise während einer Datensicherung oder bei der Skriptverarbeitung.
- Wenn alle Aktivitäten stattgefunden haben, werden IPS-Ereignisse erzeugt und Ausnahmen erstellt. Bei Ausnahmen handelt es sich um Aktivitäten, die als legitimiertes Verhalten gelten. Beispiel: Eine Richtlinie betrachtet bestimmte Skriptverarbeitungsvorgänge als illegales Verhalten. Bestimmte Systeme Ihres Entwicklungsbereichs müssen solche Aufgaben allerdings durchführen. Erlauben Sie das Erstellen von Ausnahmen für diese Systeme, damit sie weiterhin normal genutzt werden können, während die Richtlinie diese Aktivität auf anderen Systemen weiterhin verhindert. Machen Sie diese Ausnahmen zu einem Teil einer Serverrichtlinie, die nur für den Entwicklungsbereich gilt.
- Es kann auch der Fall sein, dass Sie bestimmte Softwareanwendungen besitzen, die in bestimmten Bereichen Ihres Unternehmens für normale Geschäftsvorgänge benötigt, in anderen Bereichen aber nicht zugelassen werden. Beispiel: Sie lassen Instant Messaging für die Entwicklungs- und Kundendienstabteilung zu, verhindern die Verwendung aber in der Finanz- und Personalabteilung. Sie können die Anwendung auf den Systemen in den Bereichen Entwicklung und technischer Support als vertrauenswürdig einstufen, damit Benutzer vollständigen Zugriff darauf haben.

- Die Firewall-Funktion arbeitet als Filter zwischen einem Computer und dem Netzwerk oder dem Internet. Die Firewall prüft sämtlichen eingehenden und ausgehenden Datenverkehr auf Paketebene. Beim Prüfen der einzelnen ein- oder ausgehenden Pakete kontrolliert die Firewall die Liste der Firewall-Regeln, die einen Satz von Kriterien und zugehörigen Aktionen enthält. Wenn ein Paket mit allen Kriterien einer Regel übereinstimmt, führt die Firewall die von der Regel vorgegebene Aktion durch – sie lässt das Paket entweder passieren oder sie blockiert es.

Konfigurieren von Richtlinien

Richtlinien sind die Regeln, die Sie für die einzelnen Computer eines Netzwerks festlegen, das durch Host Intrusion Prevention geschützt wird. Die auf den Client-Systemen installierten Host Intrusion Prevention-Clients rufen diese Richtlinienaktualisierungen in regelmäßigen Intervallen ab.

Wenn Sie in der Konsolenstruktur unter Verzeichnis einen Knoten auswählen, werden im Detailbereich auf der Registerkarte „Richtlinien“ die in der Host Intrusion Prevention verfügbaren Funktionen angezeigt. Dazu gehören:

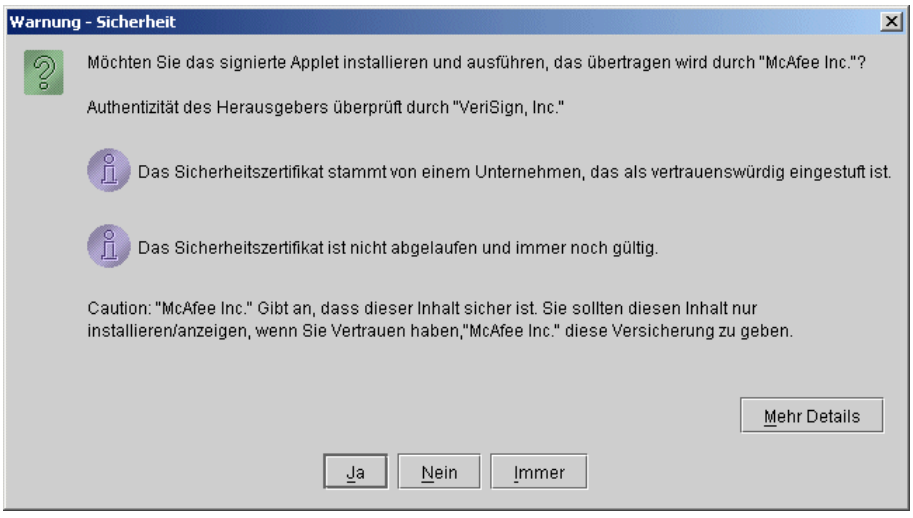
- *Allgemeine Richtlinien*
- *IPS-Richtlinien*
- *Firewall-Richtlinien*
- *Anwendungsblockierrichtlinien*

Klicken Sie auf den nach unten weisenden Pfeil, damit die für die einzelnen Funktionen verfügbaren Kategorien angezeigt werden. Einzelheiten zu den Funktionen finden Sie in den entsprechenden Abschnitten dieses Handbuchs.

Warnungen beim Anzeigen von Richtlinien

Wenn Sie Einzelheiten zu einer Host Intrusion Prevention-Richtlinie anzeigen, werden Sie möglicherweise gefragt, ob Sie ein für die Anzeige des Richtlinieninhalts erforderliches Java-Applet als vertrauenswürdig einstufen. Wenn diese Warnung angezeigt wird, klicken Sie auf **Ja** (oder auf **Immer**), um die Einzelheiten der Richtlinie anzuzeigen.

Abbildung 3-4 Java-Applet-Sicherheitswarnung


Warnung - Sicherheit
Möchten Sie das signierte Applet installieren und ausführen, das übertragen wird durch "McAfee Inc."?
Authentizität des Herausgebers überprüft durch "VeriSign, Inc."
Das Sicherheitszertifikat stammt von einem Unternehmen, das als vertrauenswürdig eingestuft ist.
Das Sicherheitszertifikat ist nicht abgelaufen und immer noch gültig.
Caution: "McAfee Inc." Gibt an, dass dieser Inhalt sicher ist. Sie sollten diesen Inhalt nur installieren/anzeigen, wenn Sie Vertrauen haben,"McAfee Inc." diese Versicherung zu geben.
Mehr Details
Ja
Nein
Immer

Einige Richtlinien für die Firewall-Funktion erfordern ein Active X-Steuerelement. Beim Öffnen einer dieser Richtlinien werden Sie möglicherweise aufgefordert, das Steuerelement auszuführen, das für die Anzeige des Richtlinieninhalts erforderlich ist. Wenn diese Warnung angezeigt wird, klicken Sie auf **Ja**, um die Einzelheiten der Richtlinie anzuzeigen.

Abbildung 3-5 Sicherheitswarnung für Active X-Steuerelement

Sicherheitswarnung
Installieren und Ausführen von "McAfee, Inc.", signiert am 14.01.2006 01:16 und herausgegeben von:
McAfee, Inc.
Authentizität des Herausgebers bestätigt durch VeriSign Class 3 Code Signing 2004 CA
Hinweis: McAfee, Inc. versichert, dass dieser Inhalt sicher ist. Die Installation bzw. das Anzeigen des Inhalts sollte nur erfolgen, wenn Sie McAfee, Inc. vertrauen.
Inhalt von McAfee, Inc. immer vertrauen
Ja
Nein
Weitere Informationen

Feineinstellung

Nach der Installation der Host Intrusion Prevention-Software sollten Sie diese dahingehend konfigurieren, dass sie den größtmöglichen Schutz bietet, ohne die Aktivitäten des Tagesgeschäfts zu beeinträchtigen. Die Standardrichtlinien in Host Intrusion Prevention passen in eine Vielzahl an Kundenumgebungen, weshalb sie auch Ihren Bedürfnissen entsprechen werden. Um Richtlinien so zu tunen, dass sie zu Ihren spezifischen Einstellungen passen, empfehlen wir die folgenden Vorgehensweisen:

- Führen Sie eine sorgfältige Definition der Sicherheitskonfiguration Ihrer Host Intrusion Prevention durch. Legen Sie fest, wer für die Konfiguration bestimmter Teile des Systems verantwortlich ist, und gewähren Sie den entsprechenden Zugriff.
- Ändern Sie die standardmäßigen Richtlinien für den IPS-Schutz oder die Firewall-Regeln, in denen Sie höhere Ebenen voreingestellter Schutzmaßnahmen einstellen können.
- Ändern Sie den Schweregrad bestimmter Signaturen. Beispiel: Wenn eine Signatur durch die tägliche Arbeit von Benutzern ausgelöst wird, dann stellen Sie den Schweregrad geringer ein. Weitere Informationen dazu finden Sie unter *Konfigurieren der Richtlinie für den IPS-Schutz* auf Seite 41.
- Konfigurieren Sie *Benachrichtigungen*, damit bei bestimmten Ereignissen bestimmte Mitarbeiter benachrichtigt werden. Beispiel: Eine Benachrichtigung kann gesendet werden, wenn auf einem bestimmten Server eine Aktivität ein Ereignis der Stufe „Hoch“ auslöst. Weitere Informationen dazu finden Sie unter *Einrichten von Benachrichtigungen für Ereignisse* auf Seite 132.

Verwenden der Hilfe

Es steht sowohl für ePolicy Orchestrator als auch für Host Intrusion Prevention eine Online-Hilfe zur Verfügung. Die ePolicy Orchestrator-Hilfe können Sie über die Schaltfläche „Hilfe“ in der ePolicy Orchestrator-Symbolleiste und über die Detailbereiche der Konsole aufrufen. In der Host Intrusion Prevention wird die Hilfe über die Hilfeschaltflächen auf der Seite **Richtlinieneinstellungen** und die zugehörigen Dialogfelder aufgerufen.

Das Fenster **Hilfe** der Host Intrusion Prevention bietet Informationen über die Richtlinie oder über das Dialogfeld, von der bzw. aus dem sie aufgerufen wurde. Über die Links **Verwandtes Thema** auf der Seite gelangen Sie zu den Anweisungen zum Ausführen bestimmter Tasks. Über das Inhaltsverzeichnis, den Index oder die Suchfunktion können Sie auf weitere Informationen zugreifen.

Vorgehensweisen für die Hilfe-Navigation

Ziel	Aktion...
Zurück zu der ursprünglich angezeigten Seite oder zu der Seite navigieren, auf der Sie auf eine Verknüpfung geklickt haben	Klicken Sie im Kontextmenü auf **Zurück**. **Hinweis:** Verwenden Sie nicht die Schaltflächen **Zurück** oder **Weiter**. Darüber navigieren Sie linear durch die Seiten des Inhaltsverzeichnisses.
Das Inhaltsverzeichnis (Index) anzeigen und aus einem einzelnen Hilfebereich suchen	Klicken Sie auf (**Navigation anzeigen**).
Kenntlich machen, wo die Seite im Inhaltsverzeichnis erscheint	Klicken Sie auf (**Im Inhalt anzeigen**). Hinweis: Einige Seiten sind hilfespezifisch und werden nicht im Inhaltsverzeichnis angezeigt.
Die Hilfe so durchblättern, wie das Inhaltsverzeichnis verläuft	Klicken Sie auf (**Zurück** und **Weiter**).
Verwandte Themen mit Anleitungen anzeigen	Klicken Sie auf (**Verwandte Themen**).
Einen Eintrag im Index finden	Klicken Sie im linken Bereich auf **Index**.
Eine Seite drucken	Klicken Sie auf (**Drucken**) oder klicken Sie im Kontextmenü auf **Drucken**.
Ein Lesezeichen einer Seite für einen HTML-Browser erstellen	Klicken Sie auf (**Lesezeichen**).
Eine Suche durchführen	Klicken Sie im Navigationsbereich auf **Suchen**, geben Sie das Wort oder die zu suchenden Wörter ein und klicken Sie auf **Los**.
Die nach einer Suche auf einer Seite vorhandene Textmarkierung entfernen	Klicken Sie im Kontextmenü auf **Aktualisieren**.

Hilfe in der Benutzeroberfläche

Eine kurze Beschreibung der Funktion einer Registerkarte oder eines Dialogfelds erscheint direkt auf der Registerkarte oder dem Dialogfeld.

Eine Beschreibung der einzelnen Schaltflächen der Symbolleiste erscheint, wenn Sie den Mauszeiger darauf positionieren. Die folgende Tabelle erläutert die in Listen enthaltenen Symbole, die für Informationen stehen:

Tabelle 3-1 Host Intrusion Prevention-Symbole

IPS-Ereignisse/Signaturen	
	Schweregrad: Informationen
	Schweregrad: Niedrig
	Schweregrad: Mittel
	Schweregrad: Hoch
	Schweregrad: Deaktiviert
IPS-Ausnahmeregeln	
	Status: Aktiviert
	Status: Deaktiviert
	Reaktion: Zulassen
	Reaktion: Blockieren
	Hinweis angehängt
IPS-Signaturregeln	
	Netzwerkintrusionsschutz
	Benutzerdefinierter Host Intrusion Prevention-Schutz
Firewall-/Quarantäne-/Anwendungsblockierregeln	
	Richtung: Eingehend
	Richtung: Ausgehend
	Richtung: Eingehend und ausgehend
	Aktion: Zulassen
	Aktion: Blockieren
	Regelübereinstimmung als Intrusion behandeln
	Regel auf definiertes Zeitintervall beschränken

4 IPS-Richtlinien

Die IPS (Intrusionspräventionssystem)-Funktion von Host Intrusion Prevention schützt Computer, die über die Host-Intrusionspräventionstechnologie verfügen. IPS-Richtlinien aktivieren und deaktivieren den IPS-Schutz, legen die Reaktionsebene für Ereignisse fest und bieten Einzelheiten zu Ausnahmen, Signaturen, Anwendungsschutzregeln, Ereignissen und vom Client erzeugten Ausnahmen.

In diesem Abschnitt wird die IPS-Funktion beschrieben. Folgende Themen werden behandelt:

- *Übersicht*
- *Konfigurieren der Richtlinie für IPS-Optionen*
- *Konfigurieren der Richtlinie für den IPS-Schutz*
- *Konfigurieren der Richtlinie für IPS-Regeln*
- *Details der IPS-Regelrichtlinien*
- *IPS-Ereignisse*
- *IPS-Client-Regeln*
- *IPS-Ausnahmeregeln suchen*

Übersicht

Host Intrusion Prevention-Clients verfügen über eine Datenbank mit IPS-Signaturregeln, die bestimmen, ob eine Aktivität auf dem Client-Computer schädlich oder harmlos ist. Wenn schädliche Aktivitäten erkannt werden, werden Warnungen, die als Ereignisse bekannt sind, an die ePO-Konsole gesendet und in der Richtlinie „IPS-Regeln für Host Intrusion Prevention“ angezeigt.

Die für Signaturen in der Richtlinie „IPS-Schutz“ festgelegte Schutzebene bestimmt, welche Aktion ein Client ergreift, wenn ein Ereignis stattfindet. Antworten oder Reaktionen umfassen das Ignorieren, Protokollieren oder Verhindern der Aktivität.

Ereignisse, die sich als falsch positiv herausstellen und aus einer legitimen Aktivität stammen, können durch das Erstellen einer Ausnahme zur Signaturregel oder durch das Einstufen von Anwendungen als „vertrauenswürdig“ überschrieben werden. Clients im adaptiven Modus erstellen automatisch Ausnahmen, so genannte Client-Regeln. Verwalter können Ausnahmen jederzeit manuell erstellen.

Die Überwachung der stattfindenden Ereignisse und die erstellten Client-Ausnahmeregeln helfen dabei, zu bestimmen, wie die Bereitstellung für den optimalen IPS-Schutz getuned werden kann.

Host- und Netzwerk-IPS-Signaturregeln

Angriffe können ein charakteristisches Zeichenmuster aufweisen. Diese Signatur kann schädliche Aktivitäten erkennen und verhindern. Beispielsweise kann eine Signatur nach der Zeichenfolge **../** in einem Web-URL suchen. Wenn die Signatur aktiviert ist und das System diese Zeichenfolge findet, wird ein Ereignis ausgelöst.

Ein signaturbasierter Ansatz mit Host- und Netzwerk-IPS-Signaturen reagiert auf die meisten Erkennungsschemata, die in der Intrusionserkennung verwendet werden, und ist ein Mechanismus, der von Host Intrusion Prevention verwendet wird. Eine Datenbank mit Signaturregeln wird mit jedem Client installiert und wird aktualisiert, wenn neue Angriffstypen erkannt werden.

Signaturen werden kategorisiert nach dem Schweregrad und der Beschreibung der Gefahr, die ein Angriff aufweist. Sie werden für spezifische Anwendungen und Betriebssysteme entworfen. Die meisten Signaturen schützen das gesamte Betriebssystem. Manche schützen dagegen bestimmte Anwendungen.

Host Intrusion Prevention bietet vorwiegend Host-IPS-Signaturen und einige zusätzliche Netzwerk-IPS-Signaturen.

HIPS

Der HIPS-Schutz befindet sich auf einzelnen Systemen, wie Servern, Arbeitsstationen oder Notebooks. Der Host Intrusion Prevention-Client realisiert den Schutz, indem er den in ein System hinein- oder aus einem System hinausfließenden Datenverkehr untersucht und das Verhalten der Anwendungen und des Betriebssystems hinsichtlich möglicher Angriffe prüft. Wenn ein Angriff erkannt wird, blockiert der Client diesen im Bereich der Netzwerksegmentverbindung oder gibt Befehle an die Anwendung oder das Betriebssystem aus, das durch den Angriff ausgelöste Verhalten zu stoppen. Ein Pufferüberlauf wird beispielsweise verhindert, indem schädliche Programme blockiert werden, die in den von einem Angriff ausgenutzten Adressraum eingefügt wurden. Die Installation von Back-Door-Programmen für Anwendungen wie den Internet Explorer wird blockiert, indem der von der Anwendung ausgegebene Befehl zum Schreiben einer Datei abgefangen und abgelehnt wird.

Vorteile von Host-IPS

- Schützt nicht nur vor einem Angriff, sondern auch gegen die Ergebnisse eines Angriffs, indem blockiert wird, dass ein Programm in eine Datei schreibt.
- Schützt Laptops gegen Angriffe, wenn sich diese außerhalb des geschützten Netzwerks befinden.
- Schützt gegen lokale Angriffe, die über CDs, Memorysticks oder Disketten in das System gelangen. Diese Angriffe sind häufig darauf ausgelegt, die Berechtigungen des Benutzers auf „Root“ oder „Administrator“ heraufzusetzen, um andere Systeme des Netzwerks zu beeinträchtigen.
- Bildet die letzte Verteidigungslinie gegen Angriffe, die andere Sicherheitstools überwunden haben.

- Verhindert interne Angriffe auf Geräte, die sich in demselben Netzwerksegment befinden, oder deren Missbrauch.
- Schützt gegen Angriffe, bei denen ein verschlüsselter Datenstrom im zu schützenden System endet, indem die entschlüsselten Daten und das Verhalten untersucht werden.
- Unabhängig von der Netzwerkarchitektur. Ermöglicht den Schutz von Systemen in veralteten oder wenig verbreiteten Netzwerkarchitekturen, wie Token Ring oder FDDI.

NIPS

Auch der NIPS-Schutz befindet sich auf einzelnen Systemen. Sämtliche Daten, die zwischen dem geschützten System und dem restlichen Netzwerk ausgetauscht werden, werden hinsichtlich eines Angriffs untersucht. Wenn ein Angriff erkannt wird, werden die verdächtigen Daten gelöscht oder deren Passieren des Systems blockiert.

Vorteile von Netzwerk-IPS

- Schützt Systeme, die sich nachgelagert in einem Netzwerksegment befinden.
- Schützt damit verbundene Server und Systeme.
- Schützt vor DoS (Denial of Service)-Angriffen gegen das Netzwerk und gegen bandbreitenorientierte Angriffe, die den Netzwerkverkehr ver- oder behindern.

Verhaltensregeln

Verhaltensregeln definieren ein Profil mit legitimer Aktivität. Eine Aktivität, die nicht dem Profil entspricht, löst das Ereignis aus. Beispielsweise kann eine Verhaltensregel besagen, dass nur ein Webserver-Vorgang auf Webdateien zugreifen kann. Wenn ein anderer Vorgang versucht, auf eine Webdatei zuzugreifen, löst diese Verhaltensregel ein Ereignis aus.

Host Intrusion Prevention kombiniert die Verwendung von Signaturregeln und hart kodierten Verhaltensregeln. Diese Hybridmethode zur Identifikation von Angriffen erkennt die bekanntesten Angriffe sowie zuvor unbekannte oder Zero-Day-Angriffe.

Vordefinierte IPS-Richtlinien

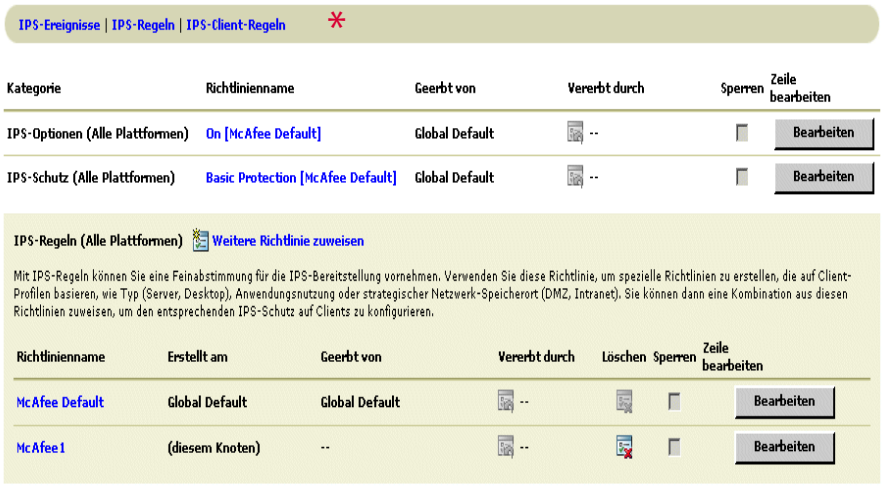
Die IPS-Funktion in Host Intrusion Prevention enthält drei Richtlinienkategorien:

- **IPS-Optionen:** Diese Richtlinie aktiviert oder deaktiviert sowohl den Host- als auch den Netzwerk-IPS-Schutz. Die vordefinierten Richtlinien umfassen **Ein (McAfee-Standard)**, **Aus**, **Adaptiv**.
- **IPS-Schutz:** Diese Richtlinie legt die Reaktion auf Ereignisse fest. Die vordefinierten Richtlinien umfassen **Grundlegend (McAfee-Standard)**, **Für erweiterten Schutz vorbereiten**, **Erweitert**, **Für maximalen Schutz vorbereiten**, **Maximaler Schutz**, **Warnung**.
- **IPS-Regeln:** Diese Richtlinie kann über eine oder mehrere Richtlinieninstanzen verfügen. Die vordefinierte Richtlinie ist die Standardrichtlinie **(McAfee-Standard)**.

Direktzugriff

Die IPS-Funktion bietet Links (*) für den Schnellzugriff auf die Überwachung und Verwaltung von IPS-Ereignissen, IPS-Regeln und IPS-Client-Regeln.

Abbildung 4-1 IPS-Funktion



Konfigurieren der Richtlinie für IPS-Optionen

Die Richtlinie **IPS-Optionen** bildet den grundlegenden Mechanismus zum Ein- und Ausschalten des IPS-Schutzes. Mit ihr wird ein Client in den adaptiven Modus versetzt und das Speichern der von ihm erstellten Ausnahmen sowie das automatische Blockieren von Netzwerkintrusionen zugelassen. Wählen Sie eine der vordefinierten Richtlinien aus oder erstellen Sie eine neue Richtlinie.

So konfigurieren Sie die Richtlinie für IPS-Optionen:

1 Erweitern Sie die **IPS**-Funktion in der Kategoriezeile **IPS-Optionen** und klicken Sie auf **Bearbeiten**.

2 Um eine voreingestellte Richtlinie anzuwenden, wählen Sie diese in der Richtlinienliste. Wenn Sie auf das Symbol des Richtliniennamens klicken, werden folgende Einstellungen angezeigt:

Wählen Sie folgende Richtlinie...	Für folgende Optionen...
(Ein (McAfee-Standard))	■ Host-IPS aktivieren ■ Netzwerk-IPS aktivieren ■ Netzwerk-Eindringlinge automatisch für 10 Minuten blockieren ■ Blockierte Hosts zurückhalten ■ Client-Regeln speichern
(Aus)	■ Blockierte Hosts zurückhalten ■ Client-Regeln speichern

Wählen Sie folgende Richtlinie...	Für folgende Optionen...
(Adaptiv)	■ Host-IPS aktivieren ■ Netzwerk-IPS aktivieren ■ Blockierte Hosts zurückhalten ■ Adaptiven Modus aktivieren ■ Client-Regeln speichern

3 Klicken Sie auf **Übernehmen**.

So erstellen Sie eine neue Richtlinie für IPS-Optionen:

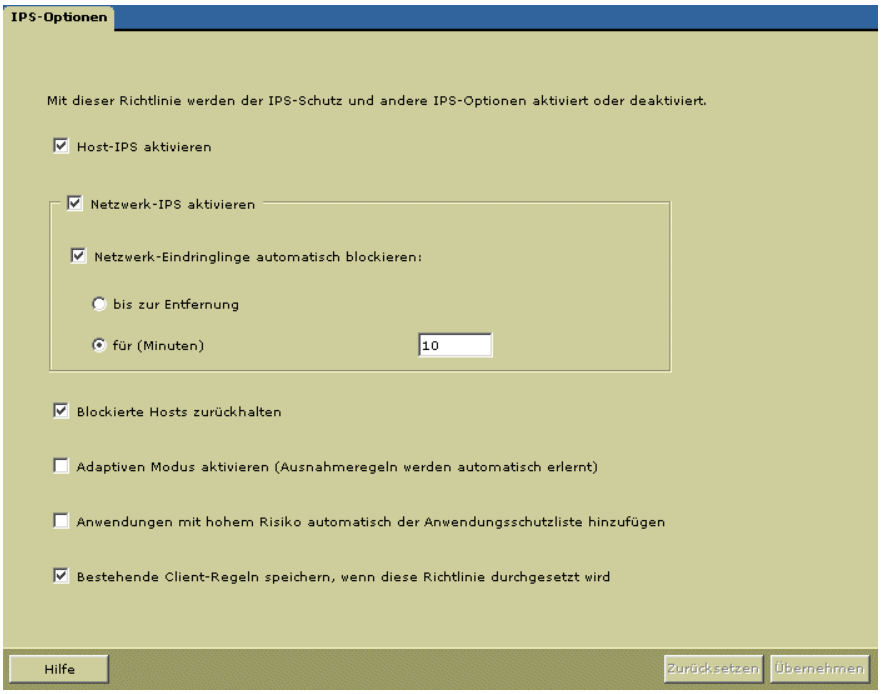
1 Klicken Sie in der Kategoriezeile **IPS-Optionen** auf **Bearbeiten** und wählen Sie in der Richtlinienliste **Neue Richtlinie**.

2 Wählen Sie im Dialogfeld **Neue Richtlinie erstellen** die Richtlinie, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein und klicken Sie auf **OK**.

Erstellen Sie eine neue duplizierte Richtlinie, wenn Sie die Einzelheiten zu einer vordefinierten Richtlinie anzeigen, indem Sie unten im Dialogfeld für die Richtlinie auf **Duplizieren** klicken. Geben Sie den Namen der neuen Richtlinie ein und geben Sie an, ob die Richtlinie augenblicklich dem aktuellen Knoten zugewiesen werden soll.

Das Dialogfeld **IPS-Optionen** wird geöffnet.

Abbildung 4-2 IPS-Optionen



3 Wählen Sie die erforderlichen Optionen aus:

Wählen Sie...	Um Folgendes zu ermöglichen...
Host-IPS aktivieren	Host-IPS-Schutz.
Netzwerk-IPS aktivieren	Netzwerk-IPS-Schutz.
Netzwerk-Eindringlinge automatisch blockieren	Ein Client, der Netzwerkintrusionsangriffe automatisch für einen bestimmten Zeitraum auf einem Host blockiert. Wählen Sie **Bis zur Entfernung**, um eingehenden und ausgehenden Verkehr auf einem Host zu blockieren, bis er manuell von einer Liste der blockierten Hosts auf dem Client entfernt wird, oder **für (Minuten)**, um den Verkehr für eine festgelegte Anzahl an Minuten zu blockieren.
Blockierte Hosts zurückhalten	Ein Client für das Blockieren eines Hosts (IP-Adresse), bis die unter **Netzwerk-Eindringlinge automatisch blockieren** festgelegten Parameter eintreffen. Wenn dies nicht ausgewählt ist, wird der Host nur bis zur nächsten Richtlinienaktualisierung blockiert.
Adaptiven Modus aktivieren	Ein Client, der Client-Regeln automatisch generiert.
Anwendungen mit hohem Risiko automatisch der Anwendungsschutzliste hinzufügen	Ein Client, der Anwendungen, in die Code eingefügt werden kann und die deshalb ein hohes Risiko darstellen, automatisch zur Liste der geschützten Anwendungen hinzufügt.
Client-Regeln speichern	Ein Client, der die Client-Regeln speichert, die er erstellt hat.

4 Klicken Sie auf **Anwenden** und anschließend auf **Schließen**.

5 Klicken Sie in der Kategoriezeile **IPS-Optionen** auf **Anwenden**.

Richtlinien können nur auf der Richtlinienkatalogseite von ePolicy Orchestrator gelöscht werden. Hierzu sind ausschließlich globale Administratoren berechtigt.

Konfigurieren der Richtlinie für den IPS-Schutz

Die Richtlinie **IPS-Schutz** legt die Schutzreaktion für Signatur-Schweregrade fest. Diese Einstellungen geben Clients vor, was zu tun ist, wenn ein Angriff oder ein verdächtiges Verhalten entdeckt wird. Jede Signatur besitzt einen von vier Schweregraden:

- **Hoch** (Rot) – Signatur von eindeutig identifizierbaren Sicherheitsbedrohungen oder schädlichen Aktionen. Diese Signaturen sind spezifisch für gut identifizierte Schwachstellen und sind in den meisten Fällen nicht verhaltensauffällig. Verhindern Sie diese Signaturen auf allen Systemen.
- **Mittel** (Orange) – Signatur einer verhaltensauffälligen Aktivität, bei der Anwendungen außerhalb ihres Bereichs arbeiten. Verhindern Sie diese Signaturen auf kritischen Systemen sowie auf Web- und SQL-Servern.
- **Gering** (Gelb) – Signatur einer verhaltensauffälligen Aktivität, bei der Anwendungen und Systemressourcen gesperrt werden und nicht geändert werden können. Wenn Sie diese Signaturen verhindern, steigert dies die Sicherheit des zugrundeliegenden Systems, es ist jedoch eine zusätzliche Feineinstellung erforderlich.

- **Information** (Blau) – Signatur einer verhaltensauffälligen Aktivität, bei der Anwendungen und Systemressourcen geändert werden, was auf ein Sicherheitsrisiko oder einen ungefährlichen Versuch hinweisen kann, auf sensible Systeminformationen zuzugreifen. Ereignisse dieser Ebene treten im Laufe der normalen Systemaktivität auf und weisen in der Regel nicht auf einen Angriff hin.

Diese Ebenen zeigen die potentiellen Gefahren für ein System an. Damit definieren Sie spezifische Reaktionen für unterschiedliche Ebenen potentieller Schäden. Sie können die Schweregrade und die Reaktionen für alle Signaturen ändern. Wenn eine verdächtige Aktivität beispielsweise wahrscheinlich keinen Schaden anrichtet, können Sie als Reaktion **ignorieren** wählen. Wenn eine Aktivität wahrscheinlich Schaden anrichtet, können Sie als Reaktion **verhindern** festlegen.

Die Richtlinie **IPS-Schutz** besitzt mehrere voreingestellte Richtlinien, die Sie auswählen können. Wenn die voreingestellten Richtlinien nicht die gewünschte Kombination der Optionen besitzt, dann erstellen Sie eine neue Richtlinie und aktivieren die entsprechenden Optionen. Die im Dialogfeld der Richtlinie **IPS-Schutz** verfügbaren Optionen hängen von der ausgewählten Richtlinie ab.

So konfigurieren Sie die Richtlinie für den IPS-Schutz:

1 Erweitern Sie die **IPS**-Funktion in der Kategoriezeile **IPS-Schutz** und klicken Sie auf **Bearbeiten**.

2 Um eine voreingestellte Richtlinie anzuwenden, wählen Sie diese in der Richtlinienliste. Wenn Sie auf das Symbol des Richtliniennamens klicken, werden folgende Einstellungen angezeigt:

Wählen Sie folgende Richtlinie...	Für folgende Optionen...
(Basisschutz (McAfee-Standard))	Verhindert Signaturen hoher Schweregrade und ignoriert die restlichen.
(Erweiterter Schutz)	Verhindert Signaturen hoher und mittlerer Schweregrade und ignoriert die restlichen.
(Maximaler Schutz)	Verhindert Signaturen hoher, mittlerer und geringer Schweregrade und protokolliert die restlichen.
(Für erweiterten Schutz vorbereiten)	Verhindert Signaturen hoher Schweregrade, protokolliert Signaturen mittlerer Schweregrade und ignoriert die restlichen.
(Für maximalen Schutz vorbereiten)	Verhindert Signaturen hoher und mittlerer Schweregrade, protokolliert Signaturen geringer Schweregrade und ignoriert die restlichen.
(Warnung)	Protokolliert Signaturen hoher Schweregrade und ignoriert die restlichen.

3 Klicken Sie auf **Übernehmen**.

So erstellen Sie eine neue Richtlinie für den IPS-Schutz:

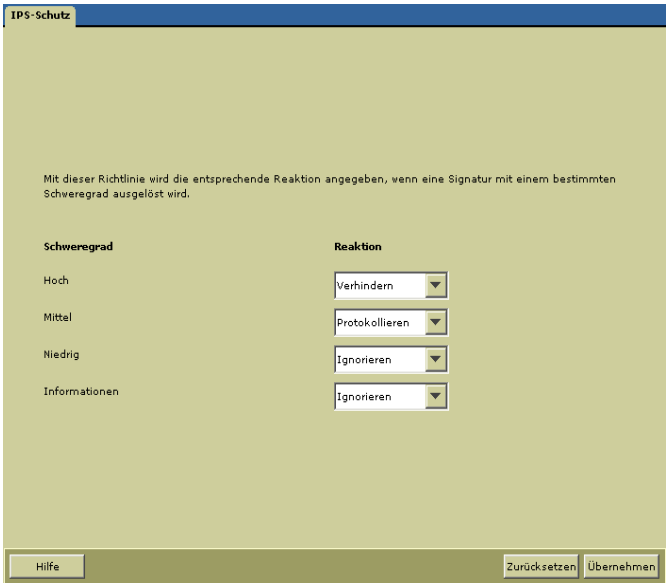
1 Klicken Sie in der Kategoriezeile **IPS-Schweregrad** auf **Bearbeiten** und wählen Sie in der Richtlinienliste **Neue Richtlinie**.

2 Wählen Sie im Dialogfeld **Neue Richtlinie erstellen** die Richtlinie, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein und klicken Sie auf **OK**.

Erstellen Sie eine neue duplizierte Richtlinie, wenn Sie die Einzelheiten zu einer vordefinierten Richtlinie anzeigen, indem Sie unten im Dialogfeld für die Richtlinie auf **Duplizieren** klicken. Geben Sie den Namen der neuen Richtlinie ein, und geben Sie an, ob die Richtlinie augenblicklich dem aktuellen Knoten zugewiesen werden soll.

Das Dialogfeld **IPS-Schutz** wird geöffnet.

Abbildung 4-3 IPS-Schutz



3 Wählen Sie den Reaktionstyp für jeden Schweregrad aus:

Für...	Wählen Sie...
Hoch	**Ignorieren**, um das Ereignis zuzulassen, ohne es zu protokollieren. **Protokollieren**, um das Ereignis zuzulassen und zu protokollieren. **Verhindern**, um das Ereignis zu verhindern und zu protokollieren.
Medium	**Ignorieren**, um das Ereignis zuzulassen, ohne es zu protokollieren. **Protokollieren**, um das Ereignis zuzulassen und zu protokollieren. **Verhindern**, um das Ereignis zu verhindern und zu protokollieren.
Niedrig	**Ignorieren**, um das Ereignis zuzulassen, ohne es zu protokollieren. **Protokollieren**, um das Ereignis zuzulassen und zu protokollieren. **Verhindern**, um das Ereignis zu verhindern und zu protokollieren.
Informationen	**Ignorieren**, um das Ereignis zuzulassen, ohne es zu protokollieren. **Protokollieren**, um das Ereignis zuzulassen und zu protokollieren.

4 Klicken Sie auf **Anwenden** und anschließend auf **Schließen**.

5 Klicken Sie in der Kategoriezeile **IPS-Schutz** auf **Anwenden**.

Richtlinien können nur auf der Richtlinienkatalogseite von ePolicy Orchestrator gelöscht werden. Hierzu sind ausschließlich globale Administratoren berechtigt.

Konfigurieren der Richtlinie für IPS-Regeln

Anders als bei den meisten anderen Richtlinienkategorien können der Richtlinie „IPS-Regeln“ mehrere Richtlinienprofile zugewiesen werden. Mithilfe dieser erweiterten Verwendung von Richtlinien können Sie mehrere Richtlinien erstellen, die der Verwendung und dem Speicherort eines Client sowie dem Typ des Systems entsprechen, auf dem er installiert ist. Damit können Sie Schutzmaßnahmen für die Intrusionsprävention einfacher anwenden. So können Sie beispielsweise für einen IIS-Server eine allgemeine Standardrichtlinie anwenden, eine Server-Richtlinie und eine IIS-Richtlinie, wobei die beiden letzten speziell für Systeme konfiguriert sind, die als IIS-Server ausgeführt werden. Neben dem Einsatz bestehender Richtlinien können Sie auch einfacher neue Richtlinien erstellen, wenn die verfügbaren Ihre Schutzanforderungen nicht mehr erfüllen.

So weisen Sie Richtlinien für IPS-Regeln zu:

1 Erweitern Sie die **IPS**-Funktion und klicken Sie in der Zeile mit dem Richtliniennamen **IPS-Regeln** auf **Bearbeiten**.

2 Um eine vorhandene Richtlinie anzuwenden, wählen Sie diese in der Richtlinienliste. Klicken Sie auf den Richtliniennamen, damit die Einzelheiten zur Richtlinie angezeigt werden.

3 Klicken Sie auf **Übernehmen**.

4 Um eine weitere Richtlinieninstanz hinzuzufügen, klicken Sie im oberen Bereich der **IPS-Regeln** auf **Weitere Richtlinie zuweisen**.

   Es wird eine neue Richtlinienzeile angezeigt.

5 Wiederholen Sie die Schritte 1 bis 3.

So erstellen Sie eine neue Richtlinie für IPS-Regeln:

1 Führen Sie einen der folgenden Vorgänge aus:

   - Klicken Sie in einer Richtliniennamenzeile **IPS-Regeln** auf **Bearbeiten**.
   - Klicken Sie oben in der Liste der „IPS-Regeln“ auf **Weitere Richtlinie zuweisen**.

2 Wählen Sie in der Richtlinienliste **Neue Richtlinie** aus.

3 Wählen Sie im Dialogfeld **Neue Richtlinie erstellen** die Richtlinie, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein und klicken Sie auf **OK**.

4 Bearbeiten Sie auf der Registerkarte **IPS-Regeln** die entsprechenden Optionen:

   - Ausnahmen (siehe *Ausnahmeregeln* auf Seite 45.)
   - Signaturen (siehe *Signaturen* auf Seite 48.)
   - Anwendungsschutzregeln (siehe *Signaturen* auf Seite 48.)

5 Klicken Sie auf **Schließen**, um das Dialogfeld für die Richtlinie **IPS-Regeln** zu schließen.

6 Klicken Sie in der Richtliniennamenzeile **IPS-Regeln** auf **Anwenden**.

Richtlinien können nur auf der Richtlinienkatalogseite von ePolicy Orchestrator gelöscht werden. Hierzu sind ausschließlich globale Administratoren berechtigt.

Details der IPS-Regelrichtlinien

Mit der Richtlinie „IPS-Regeln“ können Sie eine oder mehrere Richtlinien erstellen und anwenden, mit denen die IPS-Einstellungen definiert werden. Richtlinien sollten auf der üblichen Verwendung, dem Speicherort oder den Zugriffsrechten und Berechtigungen basieren. So können Sie einem IIS-Server z. B. eine globale Richtlinie, eine Server-Client-Richtlinie und eine IIS-Richtlinie zuweisen.

Jede Richtlinie legt folgende Punkte fest:

- *Ausnahmeregeln*
- *Signaturen*
- *Anwendungsschutzregeln*

Alle verfügbaren IPS-Richtlinien sind im Dialogfeld **Richtlinieneinstellungen** in den IPS-Regeln in der Richtlinienliste aufgeführt. Auf den ausgewählten Knoten angewendete Richtlinien werden in Fettschrift angezeigt. Klicken Sie auf **Effektive Richtlinie**, um alle für den ausgewählten Knoten geltenden Ausnahmeregeln, Signaturen und Einschluss-/Ausschlussregeln zusammen anzuzeigen.

Das Dialogfeld **Richtlinieneinstellungen** der IPS-Regeln bietet außerdem Zugriff auf folgende mit IPS-Richtlinien zusammenhängende Funktionen:

- *IPS-Ereignisse*
- *IPS-Client-Regeln*
- *IPS-Ausnahmeregeln suchen*

Ausnahmeregeln

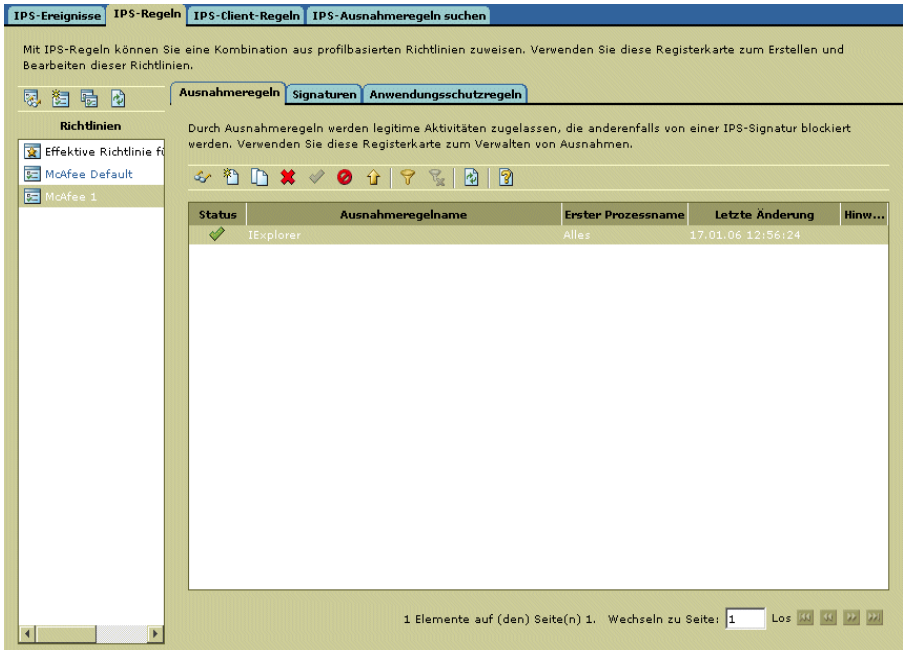
Es kann vorkommen, dass Verhaltensweisen, die normalerweise als Angriff interpretiert würden, zum normalen Arbeitsablauf eines Benutzers gehören. Diese Situation wird als *Falsch-Positiv-Warnung* bezeichnet. Um Falsch-Positiv-Warnungen zu vermeiden, können Sie eine Ausnahme für dieses Verhalten erstellen.

Mit der Ausnahmenfunktion sondern Sie Falsch-Positiv-Warnungen aus, minimieren unnötige Datenübertragungen an die Konsole und stellen sicher, dass sich Warnungen auf echte Sicherheitsbedrohungen beziehen.

Beispiel: Während des Testens von Clients erkennt ein Client die Signatur **Outlook Envelope – Verdächtiger Ausführungsmod.** Diese Signatur signalisiert, dass die E-Mail-Anwendung Outlook versucht, eine Anwendung außerhalb des üblichen Ressourcenbereichs für Outlook zu ändern. Daher verursacht ein durch diese Signatur ausgelöstes Ereignis einen Alarm, da die Möglichkeit besteht, dass Outlook eine Anwendung ändert, die üblicherweise nicht mit E-Mail-Vorgängen verbunden ist, wie z. B. **Notepad.exe**. In diesem Fall liegt der Verdacht nahe, dass ein Trojaner eingedrungen ist. Wenn der das Ereignis initiierende Prozess jedoch normalerweise für das Senden von E-Mails verantwortlich ist (um beispielsweise eine Datei mit **Outlook.exe** zu speichern), dann müssen Sie eine Ausnahme erstellen, die diese Aktion zulässt.

Im Dialogfeld **IPS-Regeln** können Sie auf der Registerkarte **Ausnahmen** eine Liste der Ausnahmen anzeigen sowie Ausnahmen erstellen und ändern.

Abbildung 4-4 IPS-Regeln – Registerkarte „Ausnahmen“



Erstellen von Ausnahmeregeln

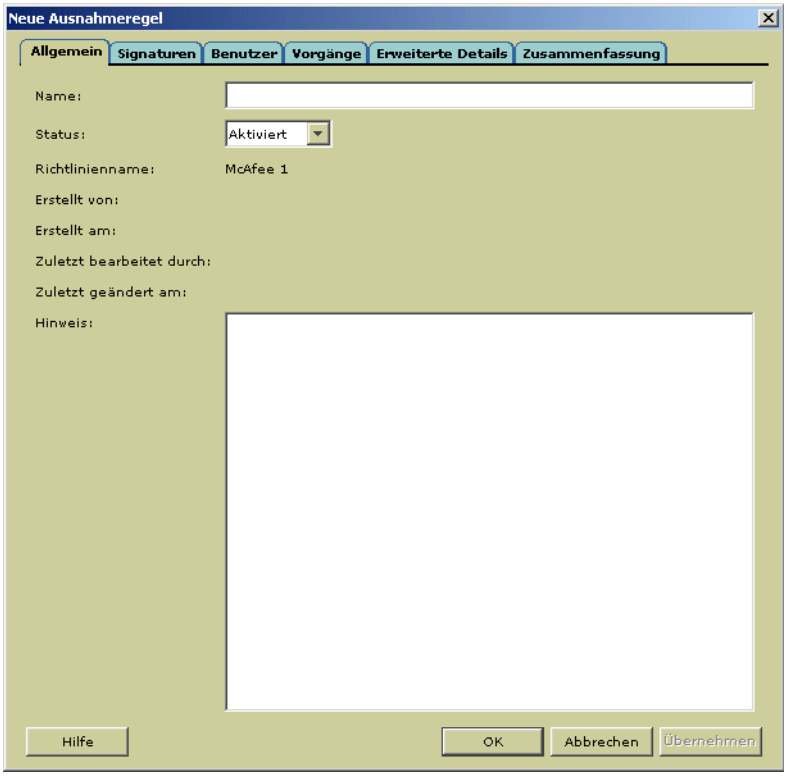
Wenn Sie eine Ausnahmeregel erstellen, müssen Sie zuerst die Ausnahme definieren und dann die Signatur angeben, für die die Ausnahme angewendet wird. Sie können eine völlig neue Ausnahme erstellen. Oder Sie nehmen das Duplikat einer vorhandenen Ausnahme oder ein Ereignis als Grundlage.

So erstellen Sie eine Ausnahme:

1 Führen Sie einen der folgenden Vorgänge aus:

- Klicken Sie auf der Registerkarte **Ausnahmeregeln** in der Symbolleiste oder im Kontextmenü auf **Erstellen**. Ein leeres Dialogfeld **Neue Ausnahme** wird geöffnet.
- Wählen Sie auf der Registerkarte **Ausnahmeregeln** eine vorhandene Ausnahme und klicken Sie in der Symbolleiste oder im Kontextmenü auf **Duplizieren**. Das vorbelegte Dialogfeld **Ausnahme duplizieren** wird geöffnet.
- Wählen Sie auf der Registerkarte **IPS-Ereignisse** das Ereignis aus, für das Sie eine Ausnahme erstellen möchten, und klicken Sie in der Symbolleiste oder im Kontextmenü auf **Ausnahme erstellen**. Wählen Sie die Richtlinie aus, in der die Ausnahme erstellt werden soll, und klicken Sie auf **OK**. Ein vorbelegtes Dialogfeld **Neue Ausnahme** wird geöffnet.

Abbildung 4-5 Dialogfeld „Neue Ausnahme“



2 Geben Sie auf allen Registerkarten die entsprechenden Daten ein und klicken Sie auf eine der folgenden Schaltflächen:

- **OK**, um die Änderungen zu speichern und das Dialogfeld zu schließen.
- **Anwenden**, um die Änderungen zu übernehmen und das Dialogfeld geöffnet zu lassen, um eine weitere Ausnahmeregel zu erstellen.
- **Abbrechen**, um die Änderungen zu löschen und das Dialogfeld zu schließen.
- **Hilfe**, um Details nachzuschlagen.

Bearbeiten von Ausnahmeregeln

Sie können Einzelheiten einer vorhandenen Ausnahme anzeigen und bearbeiten.

So bearbeiten Sie eine Ausnahmeregel:

1 Wählen Sie eine Ausnahme und klicken Sie in der Symbolleiste oder im Kontextmenü auf **Eigenschaften**. Oder doppelklicken Sie auf eine Ausnahme.

Das Dialogfeld **Ausnahmeeigenschaften** wird geöffnet.

2 Ändern Sie auf den Registerkarten die gewünschten Daten und klicken Sie anschließend auf **OK**. Klicken Sie im Dialogfeld auf **Hilfe**, um Einzelheiten anzuzeigen.

Aktivieren und Deaktivieren von Ausnahmeregeln

Anstatt nicht verwendete Ausnahmen zu löschen, können Sie diese vorübergehend deaktivieren und später dann erneut aktivieren und anwenden.

So deaktivieren/aktivieren Sie eine Ausnahme:

- Wählen Sie auf der Registerkarte **Ausnahmeregeln** eine Regel und klicken Sie in der Symbolleiste oder im Kontextmenü auf **Deaktivieren/Aktivieren**.

  Der Status der ausgewählten Ausnahme wird entsprechend geändert.

Löschen von Ausnahmeregeln

Um eine Ausnahme permanent zu löschen, wählen Sie diese auf der Registerkarte **Ausnahmeregeln** und klicken in der Symbolleiste oder im Kontextmenü auf **Löschen**. Die Ausnahme wird von der Registerkarte **Ausnahmen** entfernt.

Verschieben von Ausnahmeregeln in eine andere Richtlinie

Auf der Registerkarte **Ausnahmeregeln** können Sie eine Ausnahme problemlos von einer Richtlinie in eine andere verschieben.

So verschieben Sie eine Ausnahmeregel in eine andere Richtlinie:

1. Wählen Sie die Ausnahmeregel, die Sie verschieben möchten, und klicken Sie in der Symbolleiste oder im Kontextmenü auf **In eine andere Richtlinie verschieben**.
2. Wählen Sie in der Liste **Richtlinie auswählen** die Richtlinie aus und klicken Sie auf **OK**.

   In der ausgewählten Richtlinie wird eine Kopie der Ausnahmeregel angezeigt.

Signaturen

Signaturen beschreiben die Sicherheitsbedrohungen, Angriffsmethoden und Netzwerkintrusionen. Jede Signatur besitzt einen standardmäßigen Schweregrad, der die von einem Angriff ausgehende potentielle Gefahr beschreibt:

- **Hoch** (Rot) – Signaturen, die gegen eindeutig identifizierbare Sicherheitsbedrohungen oder schädliche Aktionen schützen. Die meisten dieser Signaturen sind spezifisch für gut identifizierte Schwachstellen und sind in den meisten Fällen nicht verhaltensauffällig. Diese Signaturen sollten auf allen Hosts verhindert werden.
- **Mittel** (Orange) – Signaturen, die stärker auf Verhaltensweisen ausgerichtet sind und verhindern, dass Anwendungen außerhalb ihrer Umgebung arbeiten (relevant für Clients beim Schutz von Webservern und Microsoft SQL Server 2000). Bei wichtigen Servern möchten Sie diese Signaturen vielleicht nach der Feineinstellung verhindern.
- **Gering** (Gelb) – Stärker auf Verhaltensweisen ausgerichtete Signaturen und Schutzschildanwendungen. Diese sperren Anwendungs- und Systemressourcen gegen Änderungen. Wenn Sie gelbe Signaturen verhindern, steigert dies die Sicherheit des zugrundeliegenden Systems, es ist jedoch eine zusätzliche Feineinstellung erforderlich.
- **Information** (Blau) – Zeigt eine Änderung der Systemkonfiguration an, was auf ein unwesentliches Sicherheitsrisiko oder einen Versuch hinweisen kann, auf sensible Systeminformationen zuzugreifen. Ereignisse dieser Ebene treten im Laufe der normalen Systemaktivität auf und weisen in der Regel nicht auf einen Angriff hin.

Signaturtypen

Die Richtlinie „IPS-Regeln" kann drei verschiedene Signaturtypen enthalten:

- **Hostsignaturen** – Standardmäßige Host-Intrusionspräventions-Signaturen (HIPS).
- **Benutzerdefinierte Hostsignaturen** – Von Ihnen erstellte benutzerdefinierte HIPS.
- **Netzwerksignaturen** – Standardmäßige Netzwerk-Intrusionspräventions-Signaturen (NIPS).

Hostsignaturen

Hostbasierte Intrusionspräventionssignaturen (HIPS) erkennen und verhindern Angriffe auf Systemvorgänge und enthalten Regeln vom Typ *Datei*, *Registrierung*, *Dienst* und *HTTP*. Diese sind von den Sicherheitsexperten der Host Intrusion Prevention entwickelt und gehören zum Produkt.

Jede Signatur besitzt eine Beschreibung und einen standardmäßigen Schweregrad. Ein Administrator mit einer entsprechenden Berechtigungsebene kann den Schweregrad einer Signatur ändern oder eine Signatur für Client-Gruppen deaktivieren.

Wenn hostbasierte Signaturen ausgelöst werden, erzeugen diese ein IPS-Ereignis, das auf der Registerkarte **IPS-Ereignisse** angezeigt wird.

Benutzerdefinierte Hostsignaturen

Benutzerdefinierte Signaturen sind hostbasierte Signaturen, die Sie erstellen können, um einen zusätzlichen Schutz für besondere Anforderungen bereitzustellen. Beispiel: Wenn Sie ein neues Verzeichnis erstellen, das wichtige Dateien enthält, können Sie zu dessen Schutz eine benutzerdefinierte Signatur erstellen.

Netzwerksignaturen

Netzwerkbasierte Intrusionspräventionssignaturen (NIPS) erkennen und verhindern bekannte netzwerkbasierte Angriffe auf das Hostsystem.

Netzwerkbasierte Signaturen werden in der Konsole in derselben Signaturliste wie die hostbasierten Signaturen angezeigt. Sie haben ihr eigenes Symbol in der Spalte **Typ** und werden im Dialogfeld **Signatureigenschaften – Allgemein** als **Netzwerk-IPS** angezeigt.

Jede Signatur besitzt eine Beschreibung und einen standardmäßigen Schweregrad. Ein Administrator mit einer entsprechenden Berechtigungsebene kann den Schweregrad einer Signatur ändern oder eine Signatur deaktivieren.

Alle netzwerkbasierten Signaturen bieten die Option, die Protokollierung abzuschalten. Dies ist auch dann möglich, wenn der Signatur durch die geltende Richtlinie als Reaktion **Protokollieren** oder **Verhindern** zugewiesen ist. Im Fall der Reaktion **Verhindern** wird der Vorgang jedoch auch dann verhindert, wenn kein Ereignis protokolliert wird.

Sie können für netzwerkbasierte Signaturen Ausnahmen erstellen – Sie können allerdings keine zusätzlichen Parameterattribute angeben, wie den Betriebssystembenutzer und den Prozessnamen. Die erweiterten Details enthalten netzwerkspezifische Parameter, wie beispielsweise die IP-Adressen, die Sie angeben können.

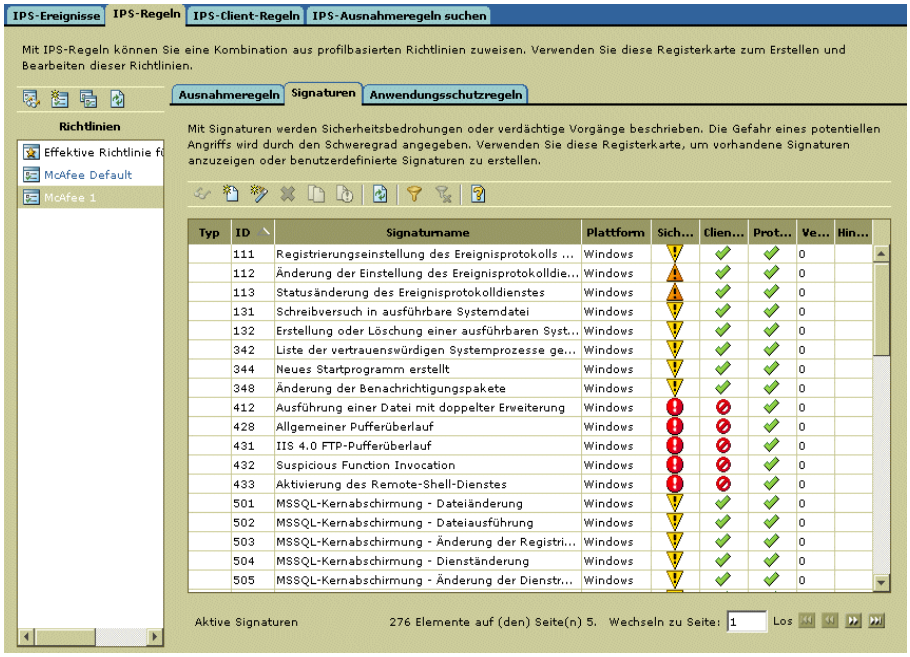
Von netzwerkbasierten Signaturen generierte Ereignisse werden zusammen mit den hostbasierten Ereignissen auf der Registerkarte **IPS-Ereignisse** angezeigt. Sie zeigen dasselbe Verhalten wie hostbasierte Ereignisse.

Netzwerkbasierte benutzerdefinierte Signaturen werden nicht unterstützt.

Anzeigen von Signaturen

Die Host Intrusion Prevention bietet drei Ansichten von Signaturen auf der Registerkarte **Signaturen**. Die Standardliste enthält nur die aktiven Signaturen. Sie können auch nur die deaktivierten Signaturen oder eine Kombination von aktiven und deaktivierten Signaturen anzeigen.

Abbildung 4-6 IPS-Regeln – Registerkarte „Signaturen“


IPS-Ereignisse
IPS-Regeln
IPS-Client-Regeln
IPS-Ausnahmeregeln suchen
Mit IPS-Regeln können Sie eine Kombination aus profilbasierten Richtlinien zuweisen. Verwenden Sie diese Registerkarte zum Erstellen und Bearbeiten dieser Richtlinien.
Ausnahmeregeln
Signaturen
Anwendungsschutzregeln
Richtlinien
Effektive Richtlinie f
McAfee Default
McAfee 1
Mit Signaturen werden Sicherheitsbedrohungen oder verdächtige Vorgänge beschrieben. Die Gefahr eines potentiellen Angriffs wird durch den Schweregrad angegeben. Verwenden Sie diese Registerkarte, um vorhandene Signaturen anzuzeigen oder benutzerdefinierte Signaturen zu erstellen.
Typ
ID
Signaturname
Plattform
Sich...
Clien...
Prot...
Ve...
Hin...
111 Registrierungseinstellung des Ereignisprotokolls ... Windows 0
112 Änderung der Einstellung des Ereignisprotokolldie... Windows 0
113 Statusänderung des Ereignisprotokolldienstes Windows 0
131 Schreibversuch in ausführbare Systemdatei Windows 0
132 Erstellung oder Löschung einer ausführbaren Syst... Windows 0
342 Liste der vertrauenswürdigen Systemprozesse ge... Windows 0
344 Neues Startprogramm erstellt Windows 0
348 Änderung der Benachrichtigungspakete Windows 0
412 Ausführung einer Datei mit doppelter Erweiterung Windows 0
428 Allgemeiner Pufferüberlauf Windows 0
431 IIS 4.0 FTP-Pufferüberlauf Windows 0
432 Suspicious Function Invocation Windows 0
433 Aktivierung des Remote-Shell-Dienstes Windows 0
501 MSSQL-Kernabschirmung - Dateiänderung Windows 0
502 MSSQL-Kernabschirmung - Dateiausführung Windows 0
503 MSSQL-Kernabschirmung - Änderung der Registri... Windows 0
504 MSSQL-Kernabschirmung - Dienständerung Windows 0
505 MSSQL-Kernabschirmung - Änderung der Dienstr... Windows 0
Aktive Signaturen
276 Elemente auf (den) Seite(n) 5. Wechseln zu Seite: 1 Los

So bearbeiten Sie die Ansicht der Signaturen:

- Klicken Sie mit der rechten Maustaste in die Signaturliste und wählen Sie die gewünschte Ansicht aus:

Wählen Sie...	Zur Anzeige von...
Aktive Signaturen anzeigen	Nur die Signaturen, die für die Richtlinie „IPS-Regeln“ aktiv sind. Dies ist die Standardansicht.
Deaktivierte Signaturen anzeigen	Nur die Signaturen, deren Schweregrad deaktiviert ist.
Alle Signaturen anzeigen	Eine Kombination von aktiven und deaktivierten Signaturen.

Ändern von Host- und Netzwerksignaturen

Die Standardsignaturen können Sie auf der Registerkarte **Signaturen** der Richtlinie **IPS-Regeln** anzeigen und bearbeiten. Dabei können Sie auch den Schweregrad der Signatur ändern, wenn die Signatur Falsch-Positiv-Meldungen auslöst.

So ändern Sie Standardsignaturen:

1 Doppelklicken Sie auf die Signatur, die Sie ändern möchten.

Das Dialogfeld **Signatureigenschaften** wird geöffnet.

2 Ändern Sie auf der Registerkarte **Allgemein** die Einstellung für die Optionen **Schweregrad**, **Client-Ausnahmen zulassen** oder **Protokollierungsstatus** und dokumentieren Sie die Änderung im Feld **Hinweise**.

3 Prüfen Sie auf der Registerkarte **Beschreibung**, was die Signatur schützt und wie sie arbeitet. Falls sich dort eine Verknüpfung befindet, klicken Sie darauf, um weitere Informationen über Sicherheitsbedrohungen im Browser anzuzeigen.

4 Klicken Sie auf **OK**.

Sie können den Schweregrad verschiedener Signaturen gleichzeitig bearbeiten, indem Sie die Signaturen auswählen und auf **Schweregrad ändern** klicken. Wählen Sie in dem angezeigten Dialogfeld **Geändert** aus sowie den neuen Schweregrad, der auf die Signaturen angewendet werden soll. Oder wählen Sie **Standard** aus, um wieder den standardmäßigen Schweregrad für die Signaturen einzustellen. Klicken Sie auf **OK**, um die Änderungen zu speichern. Die Schweregradeinstellungen lauten beispielsweise „Hoch“, „Mittel“, „Gering“, „Information“ und „Deaktiviert“.

Erstellen von benutzerdefinierten Signaturen

Mit der Host Intrusion Prevention können Sie Ihre eigenen Signaturen erstellen, verwalten und in verschiedenen Richtlinien gemeinsam nutzen. Das Erstellen benutzerdefinierter Signaturen sollte ausschließlich durch erfahrene Benutzer erfolgen. Mit benutzerdefinierten Signaturen können Sie flexibler auf Ihre Umgebung reagieren. Details hierzu finden Sie unter *Schreiben von benutzerdefinierten Signaturen* auf Seite 177.

Signaturen können nach zwei Verfahren erstellt werden:

- **Signaturerstellungsassistent** – Dies ist das einfachste Verfahren, das allerdings keine Änderung der von der Signatur geschützten Vorgänge erlaubt.
- **Standardmodus** – Dies ist das erweiterte Verfahren, mit dem Sie Vorgänge hinzufügen oder löschen können, die von der Signatur geschützt werden.

Signaturen mithilfe des Assistenten erstellen

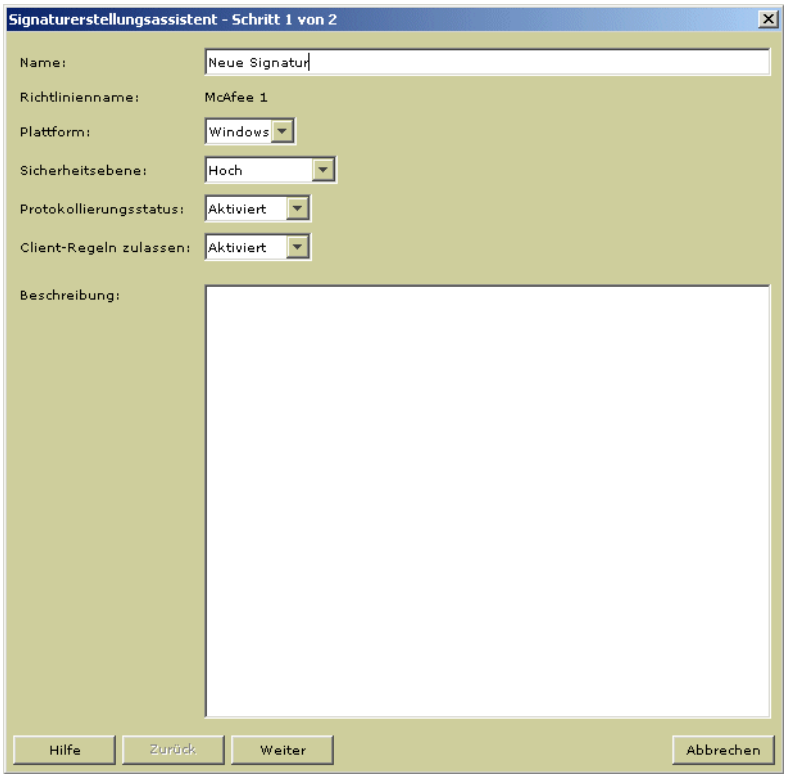
Den Signaturerstellungsassistenten sollten Sie einsetzen, wenn Sie zum ersten Mal Signaturen erstellen. Der Assistent bietet zwei Dialogfelder, in denen Sie die für die Signatur erforderlichen Informationen eingeben. Er erlaubt allerdings nicht, dass Sie von der Signatur geschützte Vorgänge ändern, hinzufügen oder löschen.

So erstellen Sie Signaturen mithilfe des Assistenten:

1 Klicken Sie in der Symbolleiste **Signatur** auf die Schaltfläche **Signaturerstellungsassistent**.

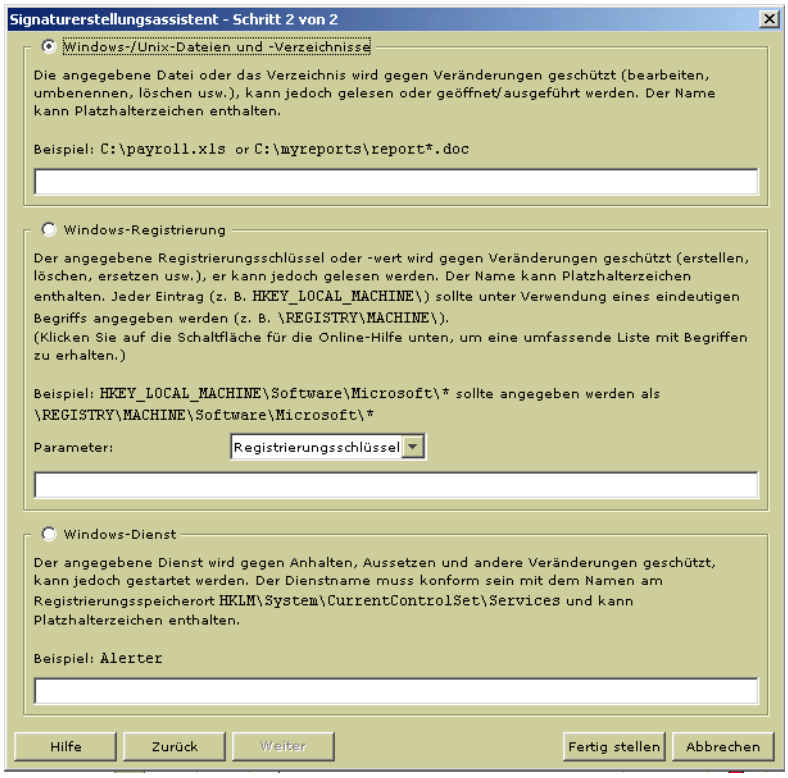
2 Geben Sie im Dialogfeld **Signaturerstellungsassistent – Schritt 1 von 2** einen Namen und eine Beschreibung ein und wählen Sie die Plattform und den Schweregrad aus. Klicken Sie anschließend auf **Weiter**.

Abbildung 4-7 Signaturerstellungsassistent – Schritt 1 von 2



3 Wählen Sie im Dialogfeld **Signaturerstellungsassistent – Schritt 2 von 2** das gegen Änderungen zu schützende Element und seine Details aus und klicken Sie dann auf **Fertig stellen**.

Abbildung 4-8 Signaturerstellungsassistent – Schritt 2 von 2


Signaturerstellungsassistent - Schritt 2 von 2
Windows-/Unix-Dateien und -Verzeichnisse
Die angegebene Datei oder das Verzeichnis wird gegen Veränderungen geschützt (bearbeiten, umbenennen, löschen usw.), kann jedoch gelesen oder geöffnet/ausgeführt werden. Der Name kann Platzhalterzeichen enthalten.
Beispiel: C:\payroll.xls or C:\myreports\report*.doc
Windows-Registrierung
Der angegebene Registrierungsschlüssel oder -wert wird gegen Veränderungen geschützt (erstellen, löschen, ersetzen usw.), er kann jedoch gelesen werden. Der Name kann Platzhalterzeichen enthalten. Jeder Eintrag (z. B. HKEY_LOCAL_MACHINE\) sollte unter Verwendung eines eindeutigen Begriffs angegeben werden (z. B. \REGISTRY\MACHINE\).
(Klicken Sie auf die Schaltfläche für die Online-Hilfe unten, um eine umfassende Liste mit Begriffen zu erhalten.)
Beispiel: HKEY_LOCAL_MACHINE\Software\Microsoft* sollte angegeben werden als \REGISTRY\MACHINE\Software\Microsoft*
Parameter:
Registrierungsschlüssel
Windows-Dienst
Der angegebene Dienst wird gegen Anhalten, Aussetzen und andere Veränderungen geschützt, kann jedoch gestartet werden. Der Dienstname muss konform sein mit dem Namen am Registrierungsspeicherort HKLM\System\CurrentControlSet\Services und kann Platzhalterzeichen enthalten.
Beispiel: Alerter
Hilfe
Zurück
Weiter
Fertig stellen
Abbrechen

Die neue Signatur wird zusammen mit einem Symbol für eine benutzerdefinierte Signatur in der Liste angezeigt.

Signaturen im Standardmodus erstellen

Dieses Verfahren sollte nur von erfahrenen Benutzern verwendet werden. Es bietet Ihnen die Möglichkeit, die von der Signatur geschützten Vorgänge auszuwählen, wobei Sie Vorgänge ändern, hinzufügen oder löschen können. Sie können eine völlig neue Signatur erstellen. Oder Sie nehmen das Duplikat einer vorhandenen benutzerdefinierten Signatur als Grundlage.

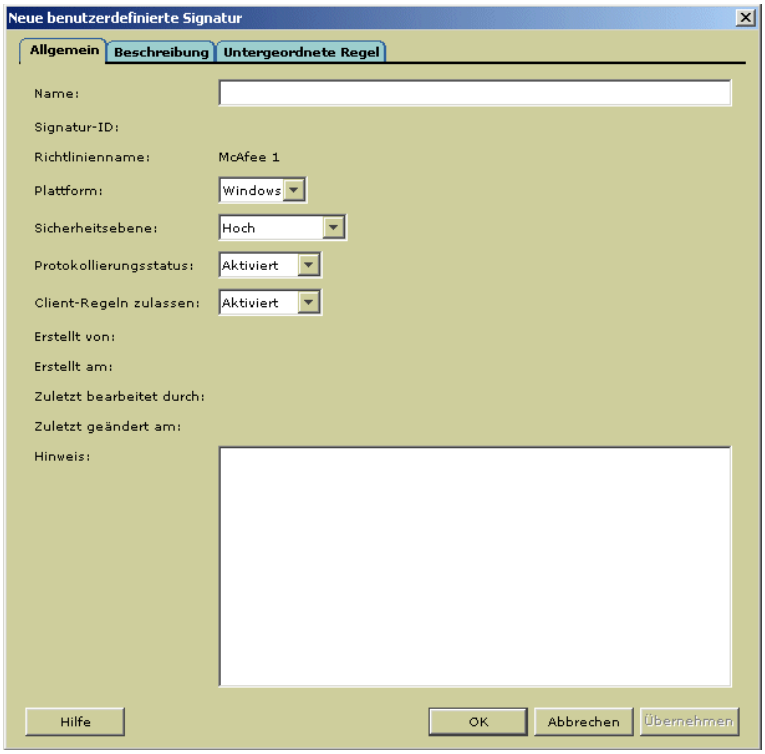
So erstellen Sie eine Signatur im Standardmodus:

1 Führen Sie einen der folgenden Vorgänge aus:

- Klicken Sie auf der Registerkarte **Signaturen** in der Symbolleiste oder im Kontextmenü auf **Erstellen**. Ein leeres Dialogfeld **Neue benutzerdefinierte Signatur** wird geöffnet.
- Wählen Sie auf der Registerkarte **Signaturen** eine benutzerdefinierte Signatur und klicken Sie in der Symbolleiste oder im Kontextmenü auf **Duplizieren**. Das vorbelegte Dialogfeld **Benutzerdefinierte Signatur duplizieren** wird geöffnet.

2 Geben Sie auf der Registerkarte **Allgemein** einen Namen ein und wählen Sie die Plattform, den Schweregrad, den Protokollierungsstatus und ob die Erstellung von Client-Regeln erlaubt werden soll.

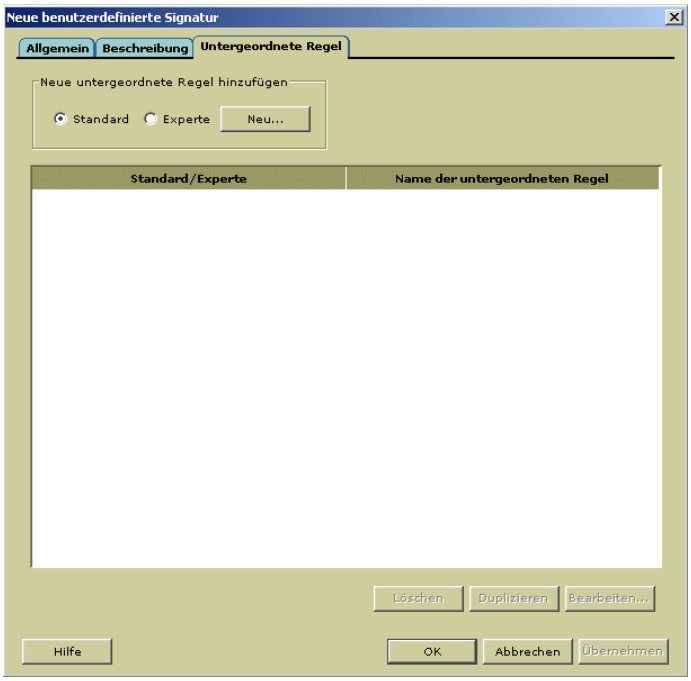
Abbildung 4-9 Neue benutzerdefinierte Signatur – Registerkarte „Allgemein“



3 Geben Sie auf der Registerkarte **Beschreibung** ein, was von der Signatur geschützt wird. Diese Beschreibung wird im Dialogfeld **IPS-Ereignis** angezeigt, wenn die Signatur ausgelöst wird.

4 Wählen Sie auf der Registerkarte **Untergeordnete Regel** entweder das **Standardverfahren** oder das **Expertenverfahren**, um die Regel zu erstellen.

Abbildung 4-10 Neue benutzerdefinierte Signatur – Registerkarte „Untergeordnete Regeln“



So verwenden Sie das Standardverfahren:	So verwenden Sie das Expertenverfahren:
Im Standardverfahren ist die Anzahl der Typen beschränkt, die in die Signaturregel aufgenommen werden können.	Im Expertenverfahren – das nur erfahrene Benutzer anwenden sollten – können Sie die Regelsyntax ohne Einschränkung der Anzahl der Typen angeben, die in die Signaturregel aufgenommen werden. Es ist wichtig, dass Sie die Regelsyntax kennen, bevor Sie beginnen, eine Regel zu schreiben. Siehe auch *Schreiben von benutzerdefinierten Signaturen* auf Seite 177.
1 Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Standardregel** wird geöffnet. 2 Geben Sie auf der Registerkarte **Allgemein** einen Namen für die Signatur ein und wählen Sie einen Typ. 3 Geben Sie auf der Registerkarte **Vorgänge** an, welche Vorgänge die ausgewählte Regel auslösen. 4 Auf der Registerkarte **Parameter** können Sie einzelne Parameter in die Regel aufnehmen oder davon ausschließen. 5 Prüfen Sie auf der Registerkarte **Regelsyntax** die für die von Ihnen gerade erstellte Signatur generierte Regelsyntax. 6 Klicken Sie auf **OK**. Die Regel wird kompiliert und die Syntax geprüft. Wenn die Signatur einen Fehler enthält und die Prüfung fehlschlägt, wird ein Dialogfeld mit einer Fehlerbeschreibung geöffnet. Sie können den Fehler dann beheben und die Regel erneut prüfen.	1 Wählen Sie im Dialogfeld **Benutzerdefinierte Signatur** auf der Registerkarte **Regeln** die Option **Experte**. 2 Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Expertenregel** wird geöffnet. 3 Geben Sie auf der Registerkarte **Allgemein** im Feld **Regelname** einen Namen für die Regel und im Feld **Hinweise** Ihre Anmerkungen zur Regel ein. 4 Geben Sie die Regel auf der Registerkarte **Regelsyntax** ein. Regeln werden im ANSI-Format und in der TCL-Syntax geschrieben. Nähere Informationen dazu finden Sie unter *Schreiben von benutzerdefinierten Signaturen* auf Seite 177. 5 Klicken Sie auf **OK**. Die Regel wird kompiliert und die Syntax geprüft. Wenn die Signatur einen Fehler enthält und die Prüfung fehlschlägt, wird ein Dialogfeld mit einer Fehlerbeschreibung geöffnet. Sie können den Fehler dann beheben und die Regel erneut prüfen.

5 Klicken Sie auf **Anwenden**, um die neuen Einstellungen anzuwenden, und dann auf **OK**.

Eine Signatur kann mehrere Regeln enthalten.

Bearbeiten von benutzerdefinierten Signaturen

Sie können benutzerdefinierte Signaturen bearbeiten und Regeln oder andere Daten hinzufügen, entfernen oder ändern.

So bearbeiten Sie eine benutzerdefinierte Signatur:

1 Doppelklicken Sie auf der Registerkarte **Signatur** auf die benutzerdefinierte Signatur, die Sie bearbeiten möchten.

Das Dialogfeld **Benutzerdefinierte Signatureigenschaften** wird geöffnet.

2 Nehmen Sie auf den Registerkarten die gewünschten Änderungen vor. Klicken Sie im Dialogfeld auf **Hilfe**, um Einzelheiten anzuzeigen.

3 Klicken Sie auf **OK**, um die Änderungen zu speichern.

Löschen von benutzerdefinierten Signaturen

Sie können benutzerdefinierte Signaturen nicht nur erstellen oder bearbeiten, sondern auch löschen. Wenn Sie eine Signatur löschen, wird auf der Registerkarte **IPS-Ereignisse** die Signatur-ID an den Namen aller von dieser Signatur ausgelösten Ereignisse angehängt.

So löschen Sie eine benutzerdefinierte Signatur:

1 Wählen Sie auf der Registerkarte **Signatur** die benutzerdefinierte Signatur, die Sie löschen möchten, und klicken Sie in der Symbolleiste oder im Kontextmenü auf **Löschen**.

2 Ein Dialogfeld wird geöffnet, in dem Sie den Löschvorgang bestätigen müssen. Klicken Sie auf **OK**.

Anwendungsschutzregeln

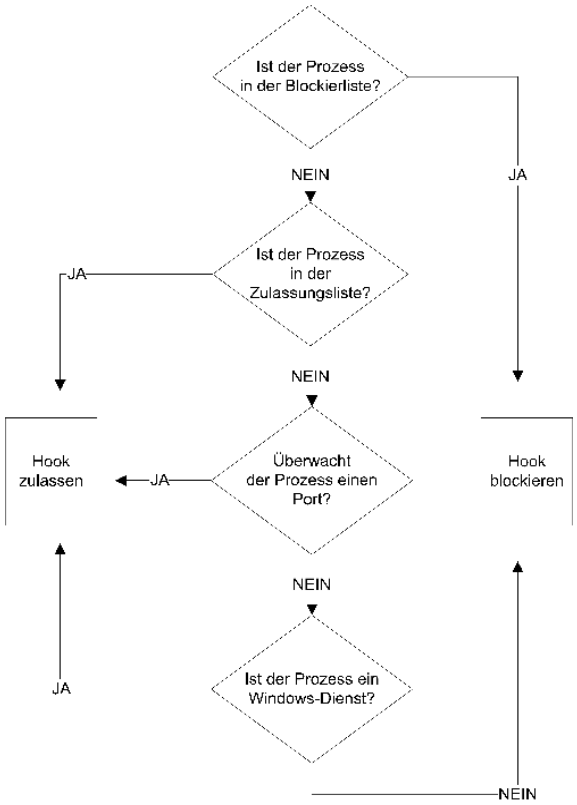
Mit Anwendungsschutzregeln verringern Sie Kompatibilitäts- und Stabilitätsprobleme im Zusammenhang mit Prozess-Hooks. Sie erlauben oder blockieren das API-Hooking auf Benutzerebene für definierte und generierte Prozesslisten. Die Datei auf Kernel-Ebene und Registrierungs-Hooks sind nicht betroffen.

Die Host Intrusion Prevention bietet eine statische Liste an Prozessen, die erlaubt oder blockiert werden. Diese Liste wird mit Inhaltsaktualisierungen aktualisiert. Darüber hinaus können für Hooks erlaubte Prozesse dynamisch zur Liste der Prozesse hinzugefügt werden, wenn die Prozessanalyse aktiviert ist. Diese Analyse findet statt:

- Jedes Mal, wenn der Client gestartet und die laufenden Prozesse durchgezählt werden.
- Jedes Mal, wenn ein Prozess gestartet wird.
- Jedes Mal, wenn die Vorgangsüberwachungsliste durch den ePolicy Orchestrator-Server aktualisiert wird.
- Jedes Mal, wenn die Liste der Prozesse, die einen Netzwerk-Port überwachen, aktualisiert wird.

Im Rahmen dieser Analyse wird zuerst geprüft, ob sich ein Prozess in der Liste der blockierten Vorgänge befindet. Wenn dies nicht der Fall ist, wird die Liste der zugelassenen Prozesse geprüft. Wenn der Prozess nicht in der Liste aufgeführt ist, wird er analysiert, um herauszufinden, ob er einen Netzwerk-Port überwacht oder als Dienst ausgeführt wird. Wenn dies nicht der Fall ist, wird er blockiert; wenn er einen Port überwacht oder als Dienst ausgeführt wird, wird er für das Erstellen von Hooks zugelassen.

Abbildung 4-11 Analyse der Anwendungsschutzregeln

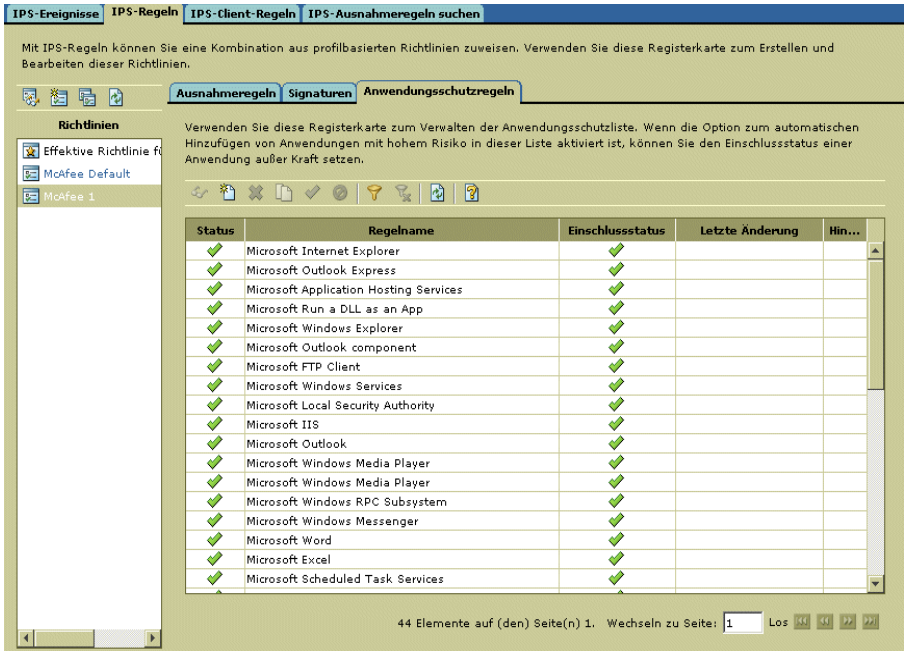


Die IPS-Komponente verwaltet einen Informations-Cache für laufende Prozesse, der die Hook-Informationen aufzeichnet. Die Firewall-Komponente ermittelt, ob ein Prozess einen Netzwerk-Port überwacht, ruft eine von der IPS-Komponente exportierte API auf und übergibt die Informationen an die API, die diese zur Überwachungsliste hinzufügt. Wenn die API aufgerufen wird, sucht die IPS-Komponente in ihrer Liste der ausgeführten Prozesse nach dem entsprechenden Eintrag. Für Prozesse ohne Hook, die sich nicht in der statischen Blockierliste befinden, wird dann ein Hook durchgeführt. Die Firewall liefert die PID (Prozess-ID), die bei der Cache-Suche nach einem Prozess als Schlüssel dient.

Mit der von der IPS-Komponente exportierten API kann die Client-UI außerdem die Liste der aktuellen Hook-Prozesse abrufen, die jedes Mal aktualisiert wird, wenn ein Prozess als Hook hinzugefügt oder entfernt wird. Ein Hook-Prozess wird entfernt, wenn die Konsole eine aktualisierte Prozessliste sendet, die angibt, dass der Hook-Prozess entfernt werden soll. Wenn die Liste der Hook-Prozesse aktualisiert wird, werden alle im Informations-Cache der laufenden Prozesse enthaltenen Prozesse mit der aktualisierten Liste verglichen. Wenn die Liste angibt, dass ein Prozess-Hook erstellt werden soll und der Prozess-Hook noch nicht existiert, dann wird der Prozess-Hook erzeugt. Wenn die Liste angibt, dass ein Prozess-Hook entfernt werden soll und der Prozess-Hook bereits existiert, dann wird der Prozess-Hook entfernt.

Die Prozess-Hooking-Listen können auf der Registerkarte **Anwendungsschutzregeln** angezeigt und bearbeitet werden. Die Client-Benutzeroberfläche zeigt, anders als die Ansicht in der Richtlinie „IPS-Regeln“, eine Liste aller Anwendungsprozesse mit einem Hook.

Abbildung 4-12 IPS-Regeln – Anwendungsschutzregeln



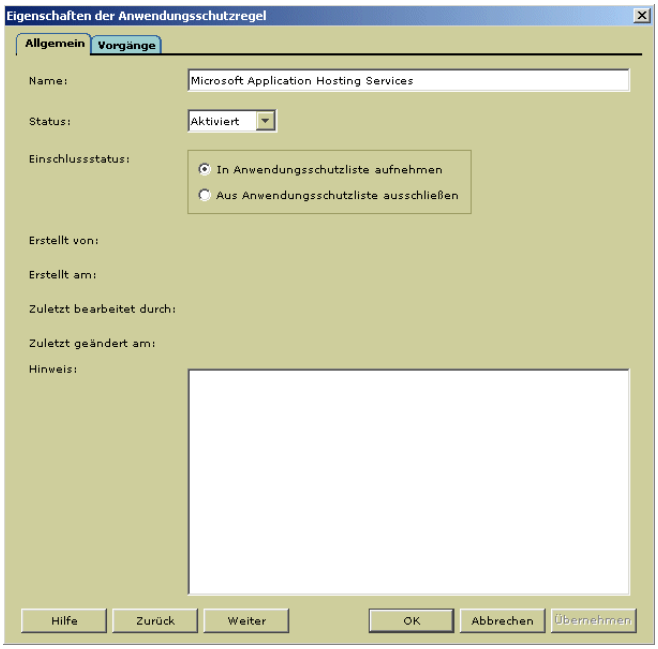
So erstellen Sie eine Anwendungsschutzregel:

1 Führen Sie einen der folgenden Vorgänge aus:

- Klicken Sie auf der Registerkarte **Anwendungsschutzregeln** in der Symbolleiste oder im Kontextmenü auf **Erstellen**. Das Dialogfeld **Neue Anwendungsschutzregel** wird geöffnet.
- Wählen Sie auf der Registerkarte **Anwendungsschutzregeln** eine Anwendung und klicken Sie in der Symbolleiste oder im Kontextmenü auf **Duplizieren**. Das vorbelegte Dialogfeld **IPS-Anwendungsschutzregeln duplizieren** wird geöffnet.

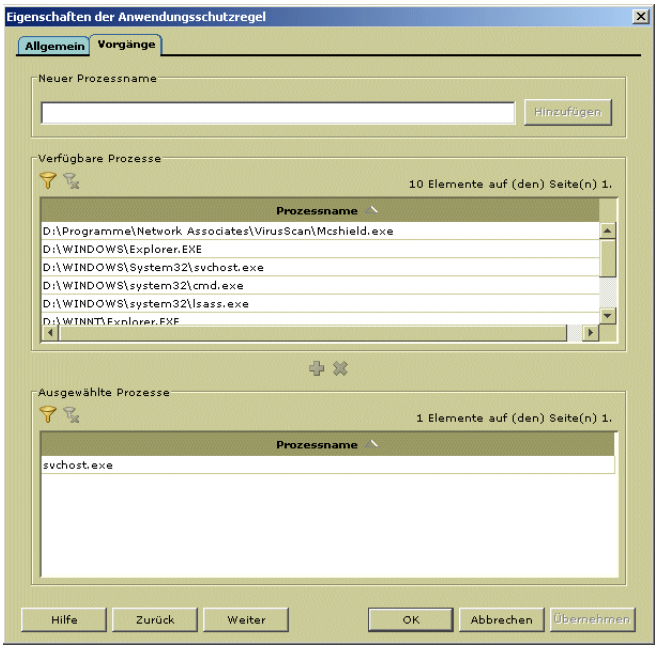
2 Geben Sie auf der Registerkarte **Allgemein** den Namen und den Status ein und legen Sie fest, ob die Anwendung einbezogen wird. Klicken Sie auf **Hilfe**, um Details nachzuschlagen.

Abbildung 4-13 Dialogfeld „Neue vertrauenswürdige Anwendung“ – Registerkarte „Allgemein“



3 Legen Sie auf der Registerkarte **Prozesse** fest, auf welche Vorgänge die Regel angewendet werden soll. Klicken Sie auf **Hilfe**, um Details nachzuschlagen.

Abbildung 4-14 Dialogfeld „Neue vertrauenswürdige Anwendung“ – Registerkarte „Allgemein“



4 Klicken Sie auf **OK**.

Bearbeiten von Anwendungsschutzregeln

Sie können die Eigenschaften einer vorhandenen Anwendungsregel anzeigen und bearbeiten, einen Einschluss- in einen Ausschlussstatus umwandeln und umgekehrt.

So bearbeiten Sie die Eigenschaften von Anwendungsregeln:

1 Wählen Sie auf der Registerkarte **Anwendungsschutzregeln** eine Anwendung aus und klicken Sie in der Symbolleiste oder im Kontextmenü auf **Eigenschaften**. Oder doppelklicken Sie auf die ausgewählte vertrauenswürdige Anwendung.

   Das Dialogfeld **Eigenschaften von Anwendungsschutzregeln** wird geöffnet.

2 Ändern Sie auf den beiden Registerkarten die gewünschten Daten, und klicken Sie anschließend auf **OK**.

Aktivieren und Deaktivieren von Anwendungsschutzregeln

Anstatt nicht verwendete Anwendungsregeln zu löschen, können Sie diese vorübergehend deaktivieren und später dann erneut aktivieren und anwenden.

So deaktivieren bzw. aktivieren Sie eine Anwendungsregel:

1 Wählen Sie auf der Registerkarte **Anwendungsschutzregeln** die aktivierte Regel, die Sie deaktivieren möchten (bzw. die deaktivierte Regel, die Sie aktivieren möchten).

2 Klicken Sie in der Symbolleiste oder im Kontextmenü auf **Deaktivieren** bzw. auf **Aktivieren**.

   Der Status der Anwendung ändert sich entsprechend auf der Registerkarte **Anwendungsschutzregeln**.

Löschen von Anwendungsschutzregeln

Um eine Anwendungsschutzregel permanent zu löschen, wählen Sie diese auf der Registerkarte **Anwendungsschutzregeln** aus und klicken Sie in der Symbolleiste oder im Kontextmenü auf **Löschen**. Die Regel wird von der Registerkarte entfernt.

IPS-Ereignisse

Ein IPS-Ereignis wird ausgelöst, sobald ein von der Signatur definierter Sicherheitsverstoß erkannt wird. Beispiel: Die Host Intrusion Prevention vergleicht den Start jeder Anwendung mit einer für diesen Vorgang zuständigen Signatur und prüft, ob es sich um einen Angriff handelt. Wenn eine Übereinstimmung vorliegt, wird ein Ereignis generiert. Wenn nicht – weil für die Signatur eventuell eine Ausnahme vorliegt oder weil die Anwendung als vertrauenswürdig eingestuft ist – wird kein Ereignis generiert.

Wenn die Host Intrusion Preventiion ein IPS-Ereignis erkennt, wird dieses auf der Registerkarte **IPS-Ereignisse** mit einem der vier Schweregrade gekennzeichnet: **Hoch**, **Mittel**, **Gering** oder **Information**.

Wenn derselbe Vorgang zwei Ereignisse auslöst, wird die höhere Reaktion ausgeführt.

Mithilfe der Liste der generierten Ereignisse können Sie bestimmen, welche Ereignisse zugelassen werden können und welche auf ein verdächtiges Verhalten hinweisen. Um Ereignisse zuzulassen, müssen Sie das System wie folgt konfigurieren:

- **Ausnahmen** – Regeln, die eine Signaturregel überschreiben. Informationen zum Erstellen einer ereignisspezifischen Ausnahme finden Sie unter *Erstellen und Anwenden der Richtlinie „Vertrauenswürdige Anwendungen“* auf Seite 120.
- **Vertrauenswürdige Anwendungen** – Lassen interne Anwendungen zu, deren Vorgänge durch eine Signatur blockiert werden könnten. Informationen zum Erstellen einer ereignisspezifischen vertrauenswürdigen Anwendung finden Sie unter *Erstellen und Anwenden der Richtlinie „Vertrauenswürdige Anwendungen“* auf Seite 120.

Mit dieser Feineinstellung können Sie auftretende Ereignisse auf ein Minimum begrenzen und so mehr Zeit für die Analyse ernster Ereignisse verfügbar machen.

Anzeigen von Ereignissen

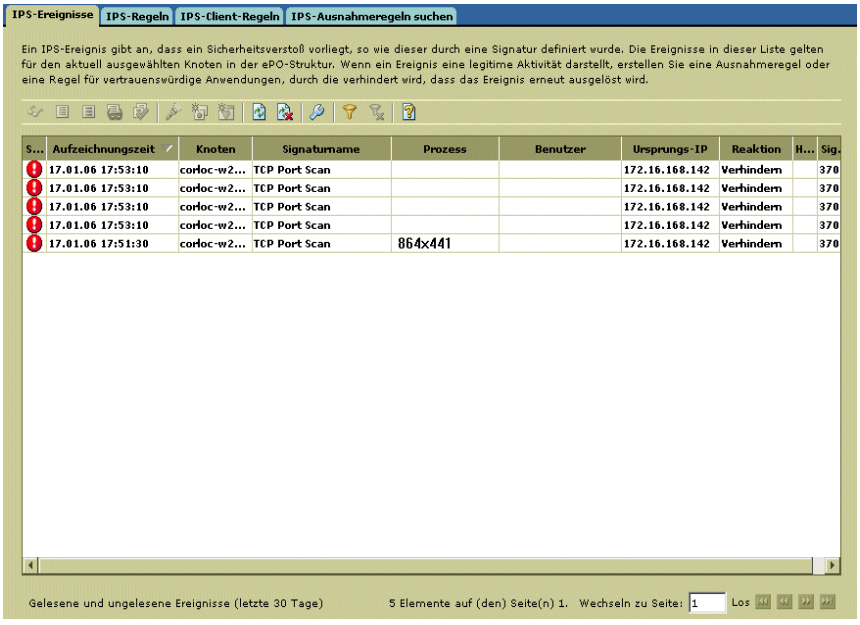
Damit Sie IPS-Ereignisse besser analysieren können, bietet Ihnen die Host Intrusion Prevention die Möglichkeit, Ereignissen drei Zustände zuzuordnen (**Ungelesen**, **Gelesen**, **Verborgen**) und diese dann in einer oder mehreren Anzeigen zu filtern.

So zeigen Sie IPS-Ereignisse an:

1 Wählen Sie in der Konsolenstruktur den Knoten, dessen IPS-Ereignisse angezeigt werden sollen.

2 Klicken Sie in der IPS-Funktion oben im Richtlinienbereich auf die Verknüpfung **IPS-Ereignisse** – falls das IPS-Managementfenster geöffnet ist, können Sie auch auf die Registerkarte **IPS-Ereignisse** klicken.

Abbildung 4-15 Registerkarte „IPS-Ereignisse“


IPS-Ereignisse
IPS-Regeln
IPS-Client-Regeln
IPS-Ausnahmeregeln suchen
Ein IPS-Ereignis gibt an, dass ein Sicherheitsverstoß vorliegt, so wie dieser durch eine Signatur definiert wurde. Die Ereignisse in dieser Liste gelten für den aktuell ausgewählten Knoten in der ePO-Struktur. Wenn ein Ereignis eine legitime Aktivität darstellt, erstellen Sie eine Ausnahmeregel oder eine Regel für vertrauenswürdige Anwendungen, durch die verhindert wird, dass das Ereignis erneut ausgelöst wird.
S... Aufzeichnungszeit Knoten Signaturname Prozess Benutzer Ursprungs-IP Reaktion H... Sig.
17.01.06 17:53:10 corloc-w2... TCP Port Scan 172.16.168.142 Verhindern 370
17.01.06 17:53:10 corloc-w2... TCP Port Scan 172.16.168.142 Verhindern 370
17.01.06 17:53:10 corloc-w2... TCP Port Scan 172.16.168.142 Verhindern 370
17.01.06 17:53:10 corloc-w2... TCP Port Scan 172.16.168.142 Verhindern 370
17.01.06 17:51:30 corloc-w2... TCP Port Scan 864x441 172.16.168.142 Verhindern 370
Gelesene und ungelesene Ereignisse (letzte 30 Tage)
5 Elemente auf (den) Seite(n) 1. Wechseln zu Seite: 1 Los

Eine Liste aller mit dem Client zusammenhängender Ereignisse wird angezeigt. Standardmäßig werden nicht alle Ereignisse angezeigt. Einzelheiten zum Konfigurieren der Ereignisansicht finden Sie unter *Konfigurieren der Ereignisansicht* auf Seite 62.

Konfigurieren der Ereignisansicht

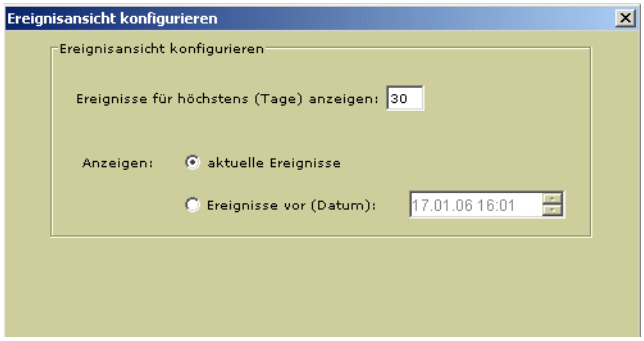
Standardmäßig werden nicht alle Ereignisse angezeigt. Standardmäßig werden nur Ereignisse für 30 Tage angezeigt. Sie können festlegen, dass die Ereignisse einer bestimmten Anzahl von Tagen angezeigt werden oder dass Ereignisse angezeigt werden, die vor einem bestimmten Datum und einer bestimmten Uhrzeit eingetreten sind.

So ändern Sie die Ereignisansicht:

1 Klicken Sie auf der Registerkarte **IPS-Ereignisse** in der Symbolleiste oder im Kontextmenü auf **Ereignisansicht konfigurieren**.

Das Dialogfeld **Ereignisansicht konfigurieren** wird geöffnet.

Abbildung 4-16 Dialogfeld „Ereignisansicht konfigurieren“



2 Geben Sie die Anzahl der Tage ein, für die Ereignisse angezeigt werden sollen.

3 Wählen Sie **Ereignisse vor (Datum)**, und geben Sie das Datum und die Uhrzeit ein, damit alle bis zu diesem Zeitpunkt eingetretenen Ereignisse angezeigt werden.

4 Klicken Sie auf **OK**.

Filtern von Ereignissen

Welche Ereignisse angezeigt werden, hängt davon ab, welche Anzeige Sie wählen. Wählen Sie im Kontextmenü den entsprechenden Befehl:

- **Alle Ereignisse anzeigen** – In dieser Anzeige werden sämtliche Ereignisse angezeigt. Gelesene Ereignisse werden in normaler Schrift angezeigt, ungelesene Ereignisse in Fettschrift, verborgene Ereignisse in grauer Schrift und verborgene aggregierte Ereignisse in hellblauer Schrift.
- **Gelesene und ungelesene Ereignisse anzeigen** – In dieser Anzeige werden alle Ereignisse angezeigt, die entweder den Status „Gelesen“ oder den Status „Ungelesen“ besitzen. Verborgene Ereignisse werden nicht angezeigt.
- **Ungelesene Ereignisse anzeigen** – In dieser Anzeige werden alle ungelesenen Ereignisse angezeigt. Diese Ereignisse werden in Fettschrift angezeigt. Gelesene und verborgene Ereignisse werden nicht angezeigt.
- **Gelesene Ereignisse anzeigen** – In dieser Anzeige werden alle gelesenen Ereignisse angezeigt. Diese Ereignisse werden in normaler Schrift angezeigt. Gelesene und verborgene Ereignisse werden nicht angezeigt.
- **Verborgene Ereignisse anzeigen** – In dieser Anzeige werden alle verborgenen Ereignisse angezeigt. Diese Ereignisse werden in grauer Schrift angezeigt.

Markieren von Ereignissen

Ereignissen wird einer von drei Zuständen zugewiesen, mit deren Hilfe die Anzeige gefiltert wird:

- **Ungelesen** – Die Standardeinstellung für alle Ereignisse. Diese zeigt an, dass das Ereignis nicht geprüft wurde. Es wird in **Fettschrift** angezeigt.
- **Gelesen** – Das Ereignis wurde geprüft und als **Gelesen** markiert. Es wird in normaler Schrift angezeigt.
- **Verborgen** – Diese Ereignisse werden aus der normalen Ereignisansicht entfernt. Sie werden so lange nur in den Ansichten **Verborgene Ereignisse** oder **Alle Ereignisse** in grauer Schrift angezeigt, bis sie wieder als **Gelesen** oder **Ungelesen** markiert werden.

Wenn Sie Ereignisse markieren, werden diese für alle mit demselben Management-Server verbundenen Benutzer markiert.

So markieren Sie ein Ereignis als gelesen:

1. Wählen Sie auf der Registerkarte **IPS-Ereignisse** die Ereignisse, die Sie als gelesen markieren möchten.
2. Klicken Sie im Kontextmenü oder in der Symbolleiste auf die Schaltfläche **Als gelesen markieren**.

   Die Schrift des Ereignisses wechselt von Fettschrift zur normalen Schrift.

So markieren Sie ein Ereignis als ungelesen:

1. Wählen Sie auf der Registerkarte **IPS-Ereignisse** die Ereignisse, die Sie als ungelesen markieren möchten.
2. Klicken Sie im Kontextmenü oder in der Symbolleiste auf die Schaltfläche **Als ungelesen markieren**.

   Die Schrift des Ereignisses wechselt von der normalen Schrift zur Fettschrift.

So verbergen Sie ein Ereignis:

1. Wählen Sie auf der Registerkarte **IPS-Ereignisse** die Ereignisse, die Sie verbergen möchten.
2. Klicken Sie im Kontextmenü oder in der Symbolleiste auf die Schaltfläche **Verbergen (Als verborgen markieren)**.

   Die ausgewählten Ereignisse werden aus der aktuellen Ansicht entfernt.
3. Um die verborgenen Ereignisse anzuzeigen, klicken Sie im Kontextmenü oder in der Symbolleiste auf **Verborgene Ereignisse anzeigen**.

So entfernen Sie Ereignisse aus der Ansicht für verborgene Ereignisse:

1. Klicken Sie im Kontextmenü oder in der Symbolleiste auf **Verborgene Ereignisse anzeigen**.

   Die verborgenen Ereignisse werden angezeigt.
2. Wählen Sie die Ereignisse, die Sie aus dieser Ansicht entfernen möchten.
3. Klicken Sie auf **Als gelesen markieren** oder auf **Als ungelesen markieren**.

   Die ausgewählten Ereignisse werden aus der Ansicht **Verborgen** entfernt.
4. Klicken Sie im Kontextmenü auf **Gelesene und ungelesene Ereignisse anzeigen** oder auf **Alle Ereignisse anzeigen**.

Ähnliche Ereignisse markieren

In Anbetracht der Vielzahl möglicher IPS-Ereignisse sollten Sie die Anzahl der angezeigten Ereignisse einschränken oder die Art der Anzeige anpassen. Dies können Sie erreichen, indem Sie bestimmte Ereignisse als gelesen, ungelesen oder verborgen markieren. Dies kann allerdings sehr aufwendig sein.

Mit der Option **Ähnliche Ereignisse als gelesen/ungelesen/verborgen markieren** können Sie in einem Schritt alle vorhandenen, Ihren Kriterien entsprechenden ähnlichen Ereignisse markieren. Nach diesem Vorgang ausgelöste neue Ereignisse werden jedoch nicht automatisch markiert.

Die von Ihnen vorgegebenen Übereinstimmungskriterien basieren auf den Attributen, die den Ereignissen zugewiesen sind. Dazu kann eine beliebige Anzahl der folgenden Attribute gehören:

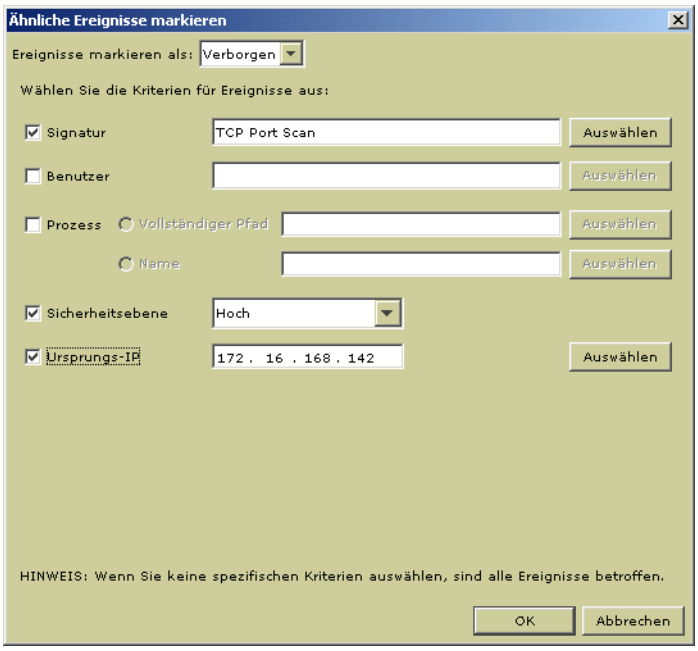
- **Agent**
- **Signaturen**
- **Benutzer**
- **Prozess**
- **Schweregrad**

So markieren Sie ähnliche Ereignisse:

1 Wählen Sie ein Ereignis und klicken Sie im Kontextmenü oder in der Symbolleiste auf **Ähnliche Ereignisse markieren**.

Das Dialogfeld **Ähnliche Ereignisse markieren** wird geöffnet.

Abbildung 4-17 Dialogfeld „Ähnliche Ereignisse markieren“



2 Wählen Sie in der Liste **Ereignisse markieren als** einen der drei Ereigniszustände: **Ungelesen**, **Gelesen** oder **Verborgen**.

3 Aktivieren Sie die Kontrollkästchen neben den Attributen, die Sie beim Markieren der Ereignisse als Kriterien verwenden möchten.

Der neben dem Kontrollkästchen angezeigte Parameterwert wird automatisch ausgewählt. Klicken Sie auf **Auswählen**, um einen anderen Parameter zu wählen. Das Dialogfeld **Auswahlliste** wird geöffnet. Wählen Sie den Parameter und klicken Sie auf **OK**.

4 Klicken Sie im ursprünglichen Dialogfeld auf **OK**. Alle mit den ausgewählten Kriterien übereinstimmenden Ereignisse werden in den ausgewählten Zustand versetzt.

Wenn Sie keine spezifischen Kriterien auswählen, sind alle Ereignisse betroffen, sobald Sie auf **OK** klicken.

Anzeigen von Ereignisdetails

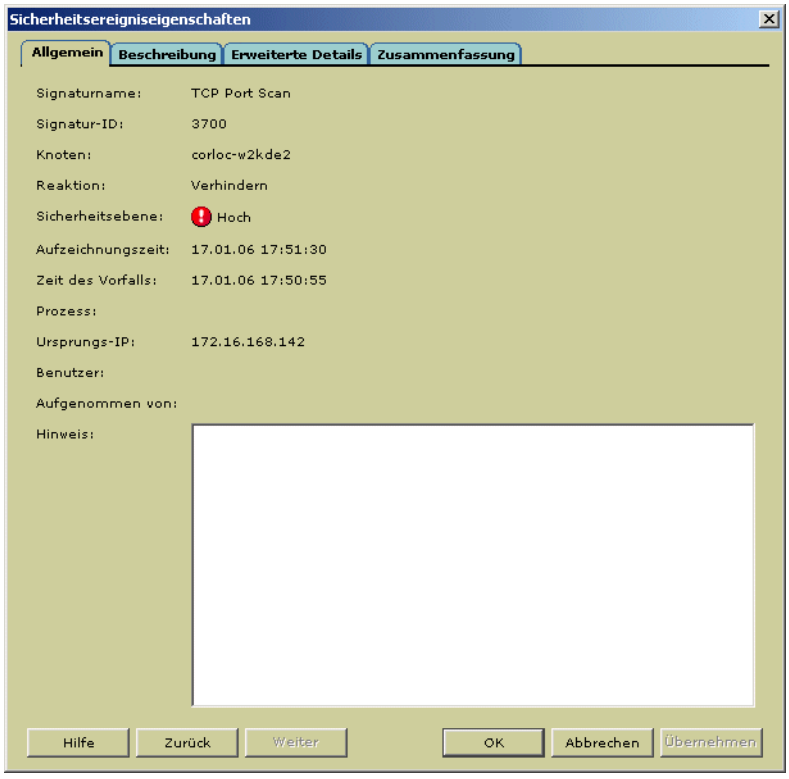
Im Dialogfeld **IPS-Ereigniseigenschaften** werden Informationen zu einem ausgewählten Ereignis angezeigt. Das Anzeigen dieser Daten kann hilfreich sein für die Feineinstellung des Systems, was es Ihnen erlaubt, eine Ausnahme oder eine vertrauenswürdige Anwendung zu erstellen oder nach bestehenden Ausnahmen auf der Grundlage des Ereignisses zu suchen.

So zeigen Sie Ereignisdetails an:

- Doppelklicken Sie auf das Ereignis, oder wählen Sie das Ereignis aus und klicken Sie im Kontextmenü oder in der Symbolleiste auf **Eigenschaften**.

Das Dialogfeld **IPS-Ereigniseigenschaften** wird geöffnet. Es enthält vier Registerkarten: **Allgemein**, **Beschreibung**, **Erweiterte Details** und **Zusammenfassung**. Klicken Sie im Dialogfeld auf **Hilfe**, um Einzelheiten anzuzeigen.

Abbildung 4-18 Dialogfeld „IPS-Ereignis“ – Registerkarte „Allgemein“



Ereignisbasierte Ausnahmen und vertrauenswürdige Anwendungen erstellen

Es kann unter bestimmten Umständen vorkommen, dass Verhaltensweisen, die als Angriff interpretiert werden, zum normalen Arbeitsablauf eines Benutzers gehören. Wenn dies der Fall ist, können Sie für dieses Verhalten eine Ausnahmeregel oder eine Regel für eine vertrauenswürdige Anwendung erstellen.

Sie können ereignisbasierte Ausnahmen oder vertrauenswürdige Anwendungen direkt für ein Ereignis erstellen, um zu verhindern, dass das entsprechende Ereignis erneut auftritt. Oder Sie können Ausnahmen oder vertrauenswürdige Anwendungen erstellen, die sich nicht auf ein bestimmtes Ereignis beziehen. Weitere Informationen zur letztgenannten Möglichkeit finden Sie unter *Ausnahmeregeln* auf Seite 45 und unter *Erstellen und Anwenden der Richtlinie „Vertrauenswürdige Anwendungen“* auf Seite 120.

Durch das Erstellen von Ausnahmen und vertrauenswürdigen Anwendungen können Sie Falsch-Positiv-Warnungen aussondern und sicherstellen, dass Sie nur aussagekräftige Benachrichtigungen erhalten.

Beispiel

Während des Testens von Clients stellen Sie fest, dass ein Client die Signatur für den E-Mail-Zugriff erkennt. Ein von dieser Signatur ausgelöstes Ereignis kann unter bestimmten Umständen alarmierend sein. Möglicherweise installieren Hacker Trojaner, die den TCP/IP-Port 25 verwenden, der in der Regel für E-Mail-Anwendungen reserviert ist. Diese Aktion würde durch die Signatur für TCP/IP-Port 25-Aktivitäten (SMTP) erkannt. Andererseits kann auch normaler E-Mail-Datenverkehr mit dieser Signatur übereinstimmen. Falls diese Signatur auftritt, müssen Sie untersuchen, welcher Prozess das Ereignis ausgelöst hat. Wenn es sich bei dem Vorgang um einen Prozess handelt, der normalerweise nicht im Zusammenhang mit E-Mails steht, wie beispielsweise Notepad.exe, müssen Sie stark davon ausgehen, dass ein Trojaner platziert wurde. Wenn der das Ereignis initiierende Prozess jedoch normalerweise für das Senden von E-Mails verantwortlich ist (Eudora, Netscape, Outlook), dann müssen Sie für dieses Ereignis eine Ausnahme erstellen.

Es kann auch vorkommen, dass Sie feststellen, dass eine bestimmte Anzahl Clients die Signatur für Programmstarts auslösen, die darauf hinweist, dass in einem der folgenden Registrierungsschlüssel ein Wert geändert oder erstellt wurde:

```
HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Run

HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/RunOnce
```

Da die in diesen Schlüsseln gespeicherten Werte Programme angeben, die beim Booten des Computers gestartet werden, kann das Erkennen dieser Signatur darauf hindeuten, dass jemand versucht, das System zu manipulieren. Es kann sich aber auch um einen harmlosen Vorgang handeln, der beispielsweise daher rührt, dass einer der Mitarbeiter auf seinem Computer **RealAudio** installiert. Bei der Installation von **RealAudio** wird der Wert **RealTray** in den Registrierungsschlüssel **Run** eingetragen.

Um zu verhindern, dass jedes Mal ein Ereignis ausgelöst wird, wenn jemand autorisierte Software installiert, müssen Sie für diese Ereignisse Ausnahmen erstellen. Danach generiert der Client für solche autorisierten Installationen keine Ereignisse mehr.

So erstellen Sie eine ereignisbasierte Ausnahme:

1 Wählen Sie ein Ereignis und klicken Sie im Kontextmenü oder in der Symbolleiste auf **Ausnahme erstellen**.

Ein vorbelegtes Dialogfeld **Neue Ausnahme** wird geöffnet.

2 Folgen Sie den Anweisungen zum Erstellen einer Ausnahme unter *Ausnahmeregeln* auf Seite 45.

So erstellen Sie eine ereignisbasierte vertrauenswürdige Anwendung:

1 Wählen Sie ein Ereignis, und klicken Sie im Kontextmenü oder in der Symbolleiste auf **Vertrauenswürdige Anwendung erstellen**.

Das vorbelegte Dialogfeld **Neue vertrauenswürdige Anwendung** wird geöffnet.

2 Folgen Sie den unter *Erstellen und Anwenden der Richtlinie „Vertrauenswürdige Anwendungen“* auf Seite 120 vorhandenen Anweisungen zum Erstellen einer vertrauenswürdigen Anwendung.

Suchen nach verknüpften Ausnahmen

Bei einem Ereignis kann es sich um eine Falsch-Positiv-Meldung handeln, was besagt, dass es sich um einen legitimen Vorgang handelt, der eine Intrusion zu sein scheint. Für Falsch-Positiv-Meldungen können Sie eine Ausnahme erstellen und die Protokollierung zukünftiger identischer Ereignisse verhindern. Vielleicht haben Sie jedoch schon verschiedene Ausnahmen für ähnliche Ereignisse erstellt. Anstatt eine neue Ausnahme zu erstellen, können Sie vielleicht eine bestehende Ausnahme bearbeiten, um sie auf das Falsch-Positiv-Ereignis anzuwenden. Das Organisieren und Geringhalten der Anzahl von Ausnahmen macht die Verwaltung einfacher.

Über die Funktion **Suchen nach verknüpften Ausnahmen** können Sie nach bestehenden Ausnahmen suchen, die mit einem oder mehreren Attributen übereinstimmen, die zu einem Ereignis gehören. Beispielsweise können Sie nach Ausnahmen suchen, die zur Signatur des Ereignisses oder Prozesses oder zu beiden Signaturen passen. Alternativ dazu können Sie auch nach Ausnahmen suchen, die bereits in dem Client bereitgestellt wurden, auf dem das Ereignis stattgefunden hat, oder nach Ausnahmen, die auf den Benutzer angewendet werden, der mit dem Ereignis verknüpft ist.

So suchen Sie nach einer verknüpften Ausnahme:

1 Wählen Sie auf der Registerkarte **IPS-Ereignisse** ein Ereignis aus, für das Sie verknüpfte Ausnahmen finden möchten, und klicken in der Symbolleiste oder im Kontextmenü auf **Suchen nach verknüpften Ausnahmen**.

Das Dialogfeld **IPS-Ausnahmeregeln suchen** mit den Suchkriterien wird angezeigt, wobei der Prozess, die Signatur und die Benutzerinformationen bereits ausgefüllt sind.

2 Wählen Sie das Kontrollkästchen für jedes Kriterium aus, das Sie anwenden möchten. Sie können die Werte bearbeiten, indem Sie auf **Bearbeiten** klicken.

3 Klicken Sie auf **OK**.

Die Registerkarte **IPS-Ausnahmen suchen** zeigt die Suchergebnisse an. Weitere Einzelheiten zur Verwendung dieser Suchfunktion finden Sie unter *IPS-Ausnahmeregeln suchen* auf Seite 70.

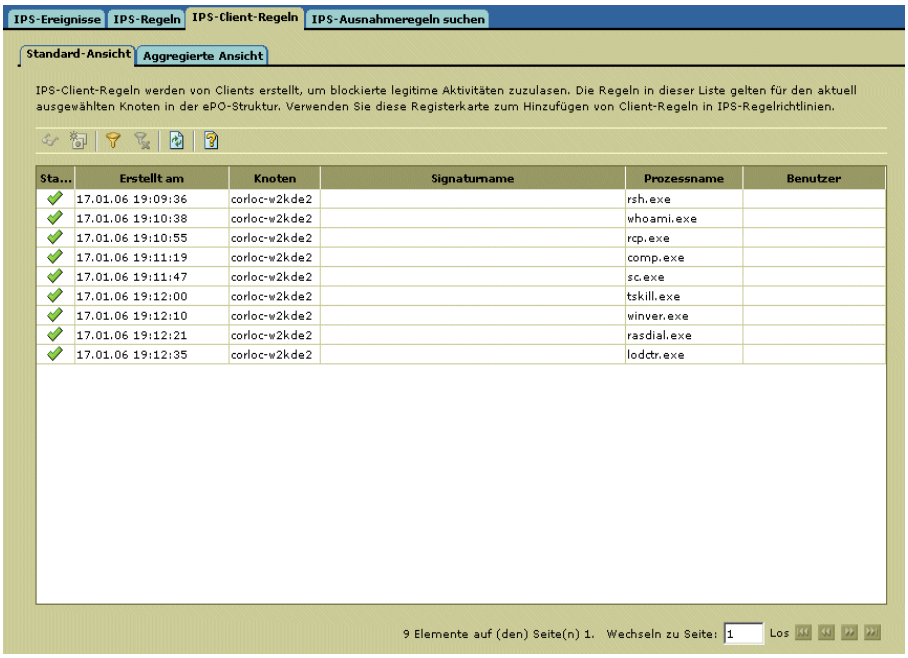
IPS-Client-Regeln

Wenn sich Clients im adaptiven Modus befinden, werden automatisch Client-Ausnahmeregeln erstellt, die Vorgänge zulassen, die ansonsten durch Administratorrichtlinien blockiert würden. Client-Regeln können auch manuell erstellt werden, vorausgesetzt, die Client-UI-Richtlinienoption für das Erlauben der manuellen Erstellung von Client-Regeln ist aktiviert. Sowohl die automatisch als auch die manuell erstellten Client-Regeln werden auf der Registerkarte **IPS-Client-Regeln** angezeigt. Client-Ausnahmeregeln, die von einem repräsentativen Client generiert werden, können auf die Registerkarte **Ausnahmeregeln** einer bestimmten Richtlinie „IPS-Regeln" migriert werden, um das Tunen einer Bereitstellung zu vereinfachen.

Standard-Ansicht

Client-Regeln erscheinen sowohl in der **Standard-Ansicht** als auch in der **Aggregierten Ansicht**. In der **Standard-Ansicht** können Sie die Regelliste sortieren und filtern, um bestimmte Ausnahmen aufzufinden und deren Details anzuzeigen. Sie können auch Client-Regeln in Server-Ausnahmeregeln einer Richtlinie **IPS-Regeln** migrieren.

Abbildung 4-19 IPS-Client-Regel – Standard-Ansicht


IPS-Ereignisse
IPS-Regeln
IPS-Client-Regeln
IPS-Ausnahmeregeln suchen
Standard-Ansicht
Aggregierte Ansicht
IPS-Client-Regeln werden von Clients erstellt, um blockierte legitime Aktivitäten zuzulassen. Die Regeln in dieser Liste gelten für den aktuell ausgewählten Knoten in der ePO-Struktur. Verwenden Sie diese Registerkarte zum Hinzufügen von Client-Regeln in IPS-Regelrichtlinien.
Sta...
Erstellt am
Knoten
Signaturname
Prozessname
Benutzer
17.01.06 19:09:36 corloc-w2kde2 rsh.exe
17.01.06 19:10:38 corloc-w2kde2 whoami.exe
17.01.06 19:10:55 corloc-w2kde2 rcp.exe
17.01.06 19:11:19 corloc-w2kde2 comp.exe
17.01.06 19:11:47 corloc-w2kde2 sc.exe
17.01.06 19:12:00 corloc-w2kde2 tskill.exe
17.01.06 19:12:10 corloc-w2kde2 winver.exe
17.01.06 19:12:21 corloc-w2kde2 rasdial.exe
17.01.06 19:12:35 corloc-w2kde2 lodctr.exe
9 Elemente auf (den) Seite(n) 1. Wechseln zu Seite: 1 Los

So migrieren Sie Client-Regeln in eine IPS-Regelrichtlinie:

1. Wählen Sie eine Client-Ausnahmeregel auf der Registerkarte **Standard-Ansicht** und klicken Sie auf **Ausnahmeregel erstellen**.
2. Wählen Sie die Richtlinie aus, auf die Sie die Client-Regel migrieren möchten, und klicken Sie auf **OK**.
3. Prüfen Sie im Dialogfeld **Ausnahmeregel** die Informationen, bearbeiten Sie sie und klicken Sie auf **OK**.

   Die neue Ausnahmeregel wird auf der Registerkarte **Ausnahmeregeln** in der Richtlinie **IPS-Regeln** angezeigt, die während des Migrationsprozesses ausgewählt wurde.

Weitere Einzelheiten finden Sie unter *Ausnahmeregeln* auf Seite 45.

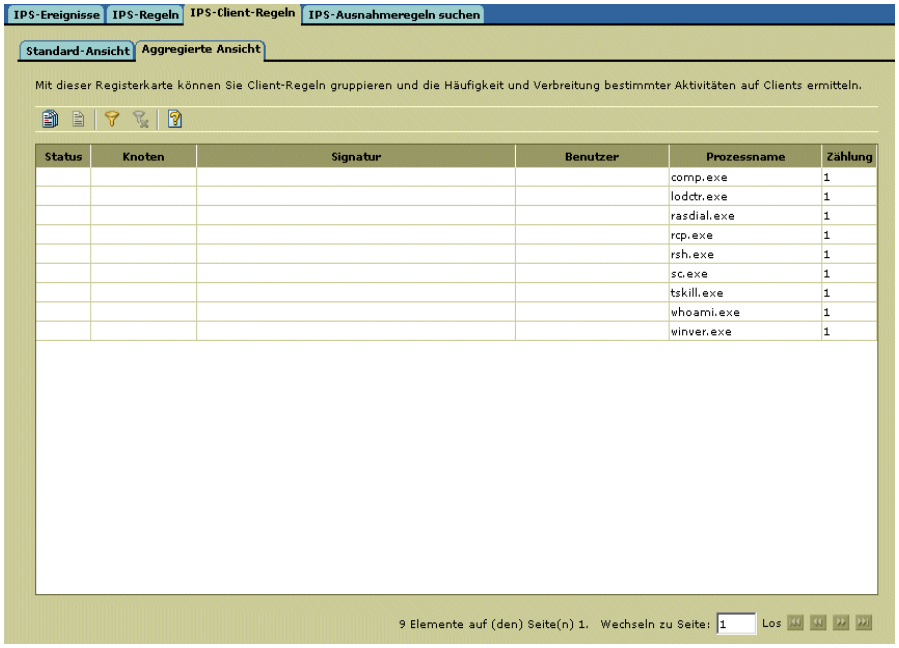
Aggregierte Ansicht

In der **Aggregierten Ansicht** können Sie Ausnahmen von der Client-Regel auf der Grundlage von Signatur, Benutzer, Prozess, Reaktion und Knoten aggregieren und so feststellen, wie oft ähnliche Ausnahmeregeln für alle Clients erstellt werden.

Die auf der Registerkarte **IPS-Client-Regeln** angezeigten Ausnahmen können Sie mit der Funktion **Aggregierte Ansicht** verwalten. In dieser Ansicht können Sie Ausnahmen mit denselben Attributen kombinieren, damit lediglich eine aggregierte Ausnahme erscheint, während Sie verfolgen können, wie oft diese Ausnahme eintritt. Anhand dieser Informationen können Sie die Feineinstellung einer Bereitstellung vornehmen und möglicherweise einige Client-Ausnahmeregeln in administrative Ausnahmeregeln überführen, um so die Anzahl der Falsch-Positiv-Meldungen für eine bestimmte Systemumgebung zu reduzieren.

Aggregierte Ausnahmen werden in blauer Schrift angezeigt und weisen in der Spalte **Zählung** eine Zahl aus. Zum Aggregieren von Ausnahmen wählen Sie beim Anzeigen der Ausnahmen Aggregierungskriterien aus.

Abbildung 4-20 IPS-Client-Regeln – Aggregierte Ansicht auf der Grundlage eines Prozesses



So aggregieren Sie Client-Regeln:

1. Klicken Sie auf der Registerkarte **IPS-Client-Regeln** auf die Registerkarte **Aggregierte Ansicht**.
2. Wählen Sie im Dialogfeld **Client-Regeln aggregieren** die Kriterien für das Aggregieren der Client-Regel-Ausnahmen. Folgende Optionen sind verfügbar: **Signatur, Benutzer, Prozess, Aktiviert, Reaktion** und **Knoten**.
3. Klicken Sie auf **OK**.

   Eine Liste der Signaturen und die Anzahl der für jede Signatur erstellten Ausnahmeregeln wird angezeigt.
4. Wählen Sie eine Zeile und klicken Sie auf **Individuelle Regeln anzeigen**, um die Details der zur Auswahl gehörenden Ausnahmeregeln anzuzeigen.

   Sie kehren zurück zur Registerkarte **Standard-Ansicht**, in der Sie die Details zu jeder Regel im aggregierten Satz sehen.

IPS-Ausnahmeregeln suchen

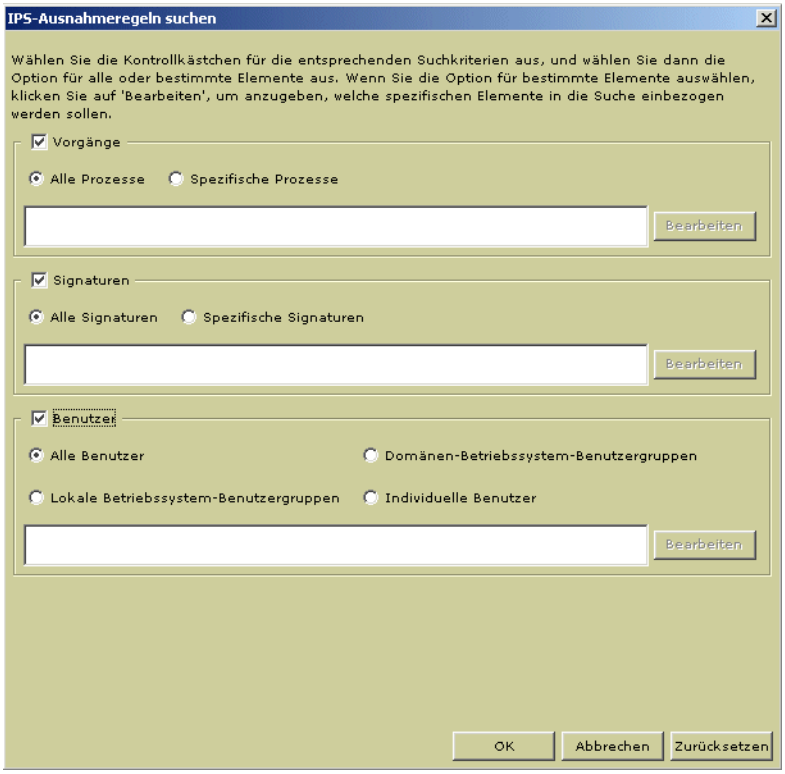
Auf der Registerkarte **IPS-Ausnahmeregeln suchen** können Sie in allen IPS-Regelrichtlinien nach Ausnahmen suchen. Mit dieser Suchfunktion können Sie bestimmen, ob eine Ausnahme für eine Signaturregel erforderlich ist. Sie ermöglicht es Ihnen außerdem, Ausnahmen zu verwalten, indem doppelte Ausnahmeregeln gelöscht oder vertrauenswürdige Anwendungen erstellt werden, um einen blockierten Prozess zu erlauben. Die Suchkriterien umfassen die Prozesse, die ein Ereignis ausgelöst haben, die Signaturen, die zum Auslösen des Ereignisses führten, und die Benutzer, die von der Ausnahmeregel betroffen waren. Wenn Sie die gesuchten Ausnahmeregeln gefunden haben, erfolgt ein Hinweis, die Liste zu verwalten, um die Anzahl der insgesamt vorhandenen Ausnahmen möglichst gering zu halten. Hierzu können Sie Ausnahmen löschen, die nicht benötigt werden, weil für bestimmte Vorgänge oder Signaturen bereits Ausnahmen bestehen. Oder Sie duplizieren eine Ausnahme und bearbeiten diese so, dass sie mehrere ähnliche Ausnahmen ersetzt. Mithilfe der Registerkarte **IPS-Ausnahmeregeln suchen** können Sie Ausnahmen auch deaktivieren, anstatt sie permanent zu löschen. Oder Sie können Ausnahmen suchen, die einem Profil entsprechen, um diese Ausnahmen dann in andere IPS-Richtinien zu kopieren.

So suchen Sie nach Ausnahmen und verwalten die Liste der Ausnahmen:

1 Klicken Sie auf der Registerkarte **IPS-Ausnahmeregeln suchen** auf **Suchen**.

Das Dialogfeld **IPS-Ausnahmeregeln suchen** wird geöffnet.

Abbildung 4-21 IPS-Ausnahmeregeln suchen



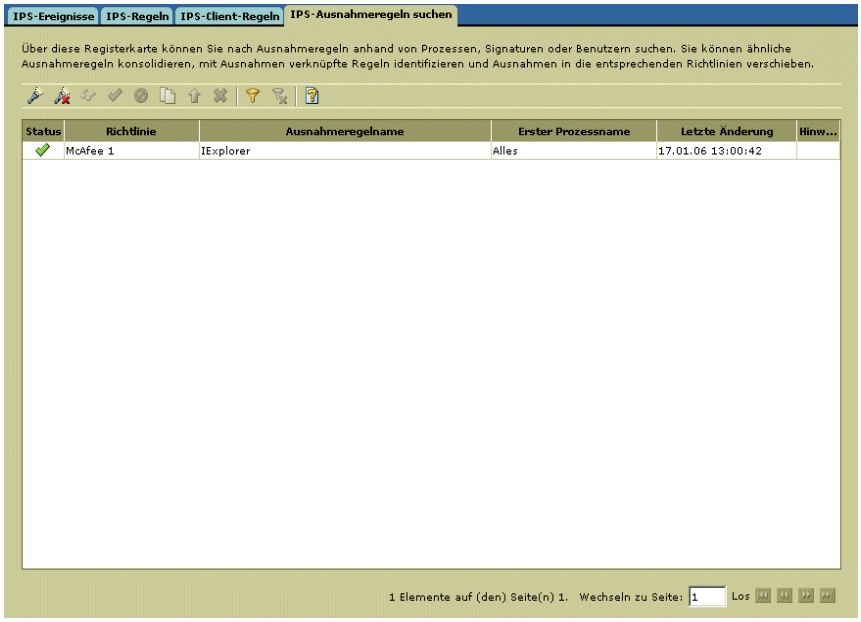
2 Wählen Sie die entsprechenden Kriterien aus und führen Sie einen der folgenden Schritte aus:

- Wählen Sie für alle Prozesse die Option **Alle** (der Standardwert).
- Wählen Sie die Option **Bestimmte** und klicken Sie auf **Bearbeiten**, um bestimmte Vorgänge anzugeben. Verschieben Sie im Dialogfeld **Nach bestimmten [Kriterien] suchen** Elemente aus der Liste der verfügbaren Kriterien in die Liste der ausgewählten Kriterien. Klicken Sie anschließend auf **OK**.

3 Klicken Sie auf **OK**.

Die Liste der mit den Suchkriterien übereinstimmenden Ausnahmen wird angezeigt.

Abbildung 4-22 Registerkarte „IPS-Ausnahmeregeln suchen“



Wenn Sie mehrere Kriterien wählen, dann stimmen die Treffer mit *beliebigen* Kriterien und nicht unbedingt mit *allen* Kriterien überein. Beispiel: Wenn Sie zwei spezifische Vorgänge gewählt haben, dann entsprechen die Ausnahmen entweder einem oder beiden Vorgängen. Es werden nicht nur Treffer angezeigt, die ausschließlich beiden Kriterien entsprechen.

4 Wählen Sie eine Ausnahme in der Liste aus und verwenden Sie Befehle aus dem Kontextmenü oder der Symbolleiste, um sie zu aktivieren/deaktivieren, verschieben Sie sie von einer Richtlinie in eine andere, erstellen Sie eine neue Ausnahme, indem Sie sie duplizieren, oder löschen Sie sie. Weitere Einzelheiten finden Sie unter *Ausnahmeregeln* auf Seite 45.

5 Firewall-Richtlinien

Die Firewall-Funktion der Host Intrusion Prevention schützt Computer, indem der gesamte Datenverkehr des Netzwerkes gefiltert wird – legitimierte Datenströme dürfen die Firewall passieren, alle anderen werden blockiert. Dies wird über Firewall-Richtlinien erreicht. In der aktuellen Version des Produkts wurden die statusbehaftete Filterung und Inspizierung für die Verwaltung von Clients der Version 6.1 hinzugefügt. Statische Legacy-Firewall-Regeln, als HIP 6.0-Regeln bezeichnet, sind ebenfalls verfügbar, gelten jedoch nur für Clients der Version 6.0. Um den Übergang von statischen zu statusbehafteten Regeln zu erleichtern, ist ein Dienstprogramm für die Migration von Firewall-Regeln verfügbar.

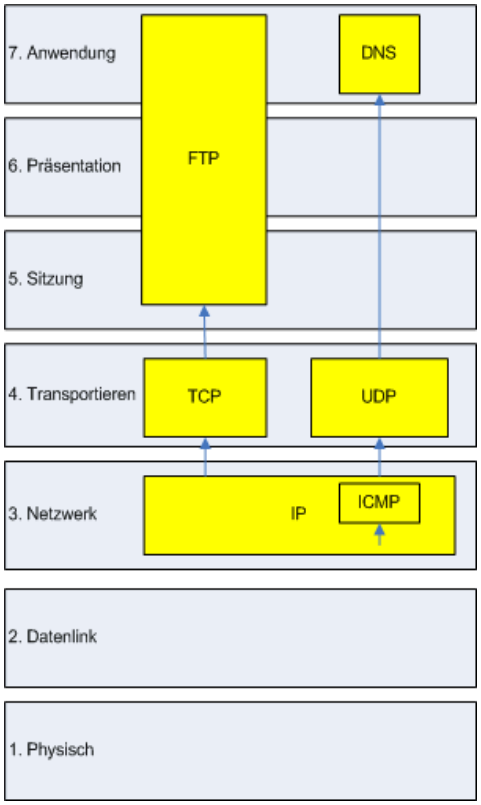
In diesem Abschnitt wird die Funktion „Firewall“ beschrieben. Folgende Themen werden behandelt:

- *Übersicht*
- *Konfigurieren der Richtlinie für Firewall-Optionen*
- *Konfigurieren der Richtlinie für Firewall-Regeln*
- *Konfigurieren der Richtlinie für Quarantäneoptionen*
- *Konfigurieren der Richtlinie „Quarantäneregeln“*

Übersicht

Die Host Intrusion Prevention-Firewall schützt einen Computer im Netzwerk vor Intrusionen, die Daten, Anwendungen oder das Betriebssystem gefährden. Sie bietet diesen Schutz, indem sie auf verschiedenen Ebenen der Netzwerkarchitektur aktiv ist, wobei verschiedene Kriterien angewendet werden, um den Netzwerkverkehr zu beschränken. Diese Netzwerkarchitektur baut auf einem Open System Interconnection (OSI)-Modell mit sieben Ebenen auf, wobei jede Ebene spezifische Netzwerkprotokolle verarbeitet.

Abbildung 5-1 Netzwerkebenen und -protokolle



HIP 6.0-Regeln

Die Firewall in Host Intrusion Prevention 6.0 basierte hauptsächlich auf der Netzwerkebene 3 und der Transportebene 4, sodass Netzwerkpakete zu ihrem Ziel weitergeleitet wurden. Auf diesen Ebenen verwendet die Firewall statische Paketfilterung mit einer Regelübereinstimmung von oben nach unten. Wenn ein Paket analysiert wird und es mit einer Firewall-Regel übereinstimmt, werden Kriterien wie die IP-Adresse, die Portnummer und der Pakettyp angewendet, um das Paket zu erlauben oder zu blockieren. Wenn keine übereinstimmende Regel gefunden wird, wird das Paket verweigert. Es sind bidirektionale Firewall-Regeln erforderlich, besonders für UDP- und ICMP-Protokolle.

HIP 6.1-Regeln

Die Firewall in Host Intrusion Prevention 6.1 verwendet erstmals eine statusbehaftete Firewall sowohl mit statusbehafteter Paketfilterung als auch mit statusbehafteter Paketinspizierung.

Statusbehaftete Paketfilterung

Die statusbehaftete Paketfilterung ist die statusbehaftete Nachverfolgung der TCP-/UDP-/ICMP-Protokollinformationen auf Transportebene 4 und darunter im OSI-Netzwerkstapel. Jedes Paket wird geprüft, und wenn das inspizierte Paket mit einer bestehenden Firewall-Regel übereinstimmt, wird das Paket erlaubt, und es wird ein Eintrag in einer Statustabelle vorgenommen. Die Statustabelle verfolgt dynamisch Verbindungen, die zuvor mit einem statischen Regelsatz abgeglichen wurden, und spiegelt den aktuellen Verbindungsstatus der TCP-/UDP-/ICMP-Protokolle wider. Wenn ein inspiziertes Paket mit einem bestehenden Eintrag in der Statustabelle übereinstimmt, wird das Paket ohne weitere Analysen erlaubt. Wenn eine Verbindung geschlossen ist oder ein Timeout vorliegt, wird der entsprechende Eintrag aus der Statustabelle entfernt.

Statusbehaftete Paketinspizierung

Die statusbehaftete Paketinspizierung ist der Prozess der statusbehafteten Paketfilterung und des Nachverfolgens von Befehlen auf der Anwendungsebene 7 des Netzwerkstapels. Diese Kombination bietet eine klare Definition des Verbindungsstatus des Computers. Der Zugriff auf die Befehle auf der Anwendungsebene bietet eine fehlerfreie Inspizierung und Sicherung von FTP-, DHCP- und DNS-Protokollen.

Host Intrusion Prevention 6.0-Clients verwenden nur die statische Firewall, sogar wenn sie in einer gemischten Umgebung mit Host Intrusion Prevention 6.1-Servern und -Clients fungieren. Um die statusbehaftete Firewall zu verwenden, müssen Sie den Client von Version 6.0 auf Version 6.1 aktualisieren. Um das Upgrade zu erleichtern, können Sie bestehende statische Regeln mithilfe des Firewall-Regelmigrators in statusbehaftete Regeln umwandeln. Siehe *Migration von benutzerdefinierten 6.0-Firewall-Regeln zu 6.1-Regeln* auf Seite 83.

Statustabelle

Eine Funktion einer statusbehafteten Firewall ist eine Statustabelle, die Informationen zu aktiven Verbindungen dynamisch speichert, die durch Regeln für das Erlauben erstellt wurden. Jeder Eintrag in der Tabelle definiert eine Verbindung auf der Grundlage folgender Faktoren:

- Protokoll: Der vordefinierte Weg, wie ein Dienst mit einem anderen kommuniziert; dies umfasst auch TCP-, UDP- und ICMP-Protokolle.
- IP-Adressen von lokalen und Remote-Computern: Jedem Computer wird eine eindeutige IP-Adresse zugewiesen, wobei es sich um eine 32-Bit-Nummer in vier Blöcken mit je acht Bit in einer Dezimalzahl mit Punkten dazwischen handelt, wie beispielsweise 192.168.1.100.
- Portnummern von lokalen und Remote-Computern: Ein Computer sendet und empfängt Dienste unter Verwendung nummerierter Ports. Der HTTP-Dienst steht typischerweise auf Port 80 zur Verfügung und die FTP-Dienste auf Port 21. Die Portnummern reichen von 0 bis 65535.
- Prozess-ID (PID): Ein eindeutiges Erkennungsmerkmal für den Prozess, der mit dem Verkehr einer Verbindung verknüpft ist.

- Zeitstempel: Die Zeit des letzten eingehenden oder ausgehenden Pakets, das mit der Verbindung verknüpft ist.
- Timeout: Die zeitliche Grenze (in Sekunden), die in der Richtlinie „Firewall-Optionen" festgelegt ist und nach der der Eintrag aus der Tabelle entfernt wird, wenn kein Paket empfangen wird, das mit der Verbindung übereinstimmt. Das Timeout für TCP-Verbindungen wird nur erzwungen, wenn die Verbindung nicht eingerichtet ist.
- Richtung: Die Richtung (eingehend oder ausgehend) des Verkehrs, der diesen Eintrag ausgelöst hat. Nachdem eine Verbindung eingerichtet wird, wird der bidirektionale Verkehr sogar mit unidirektionalen Regeln erlaubt, vorausgesetzt, der Eintrag stimmt mit den Parametern der Verbindung in der Statustabelle überein.

Funktion „Statustabelle"

- Wenn die Firewall-Regeleinstellungen sich ändern, werden alle aktiven Verbindungen gegen den neuen Regelsatz geprüft. Wenn keine übereinstimmende Regel gefunden wird, wird der Verbindungseintrag aus der Statustabelle entfernt.
- Wenn ein Adapter eine neue IP-Adresse empfängt, erkennt die Firewall die neue IP-Konfiguration und verweigert alle Einträge in der Statustabelle aufgrund einer ungültigen lokalen IP-Adresse.
- Alle Einträge in der Statustabelle, die mit einem Prozess verknüpft sind, werden gelöscht, wenn der Prozess abgeschlossen ist.

Funktionsweise von Firewall-Regeln

Firewall-Regeln bestimmen, wie Netzwerkverkehr verarbeitet wird. Jede Regel bietet einen Satz an Bedingungen, die der Verkehr erfüllen muss, und ist mit einer Aktion verknüpft: entweder Verkehr *erlauben* oder *blockieren*. Wenn die Host Intrusion Prevention Datenverkehr findet, der einer Regelbedingung entspricht, dann wird die verknüpfte Aktion durchgeführt.

Die Host Intrusion Prevention wendet Regeln nach *Vorrang* an: Die am Anfang der Firewall-Regelliste stehenden Regeln werden zuerst angewendet.

Bei domänenbasierten und Kabellos-Regeln behandelt Host Intrusion Prevention den Vorrang anders. Wenn eine Regel eine Remote-Adresse als Domänenname oder eine kabellose 802.11-Verbindung angibt, wird sie zuerst angewendet, unabhängig von ihrer Position in der Regelliste.

Wenn der Datenverkehr die Bedingungen dieser Regel erfüllt, erlaubt Host Intrusion Prevention diesen Datenverkehr oder blockiert ihn. Es werden keine weiteren in der Regelliste enthaltenen Regeln geprüft.

Wenn der Datenverkehr die Bedingung der ersten Regel jedoch nicht erfüllt, prüft die Host Intrusion Prevention die nächste in der Liste enthaltene Regel. So arbeitet das Programm die Firewall-Regelliste weiter ab, bis eine Regel gefunden wird, die der Datenverkehr erfüllt. Wenn keine Regel erfüllt ist, blockiert die Firewall den Datenverkehr automatisch. Wenn der Lernmodus aktiviert ist, wird eine Eingabeaufforderung bezüglich der einzuleitenden Aktion angezeigt. Wenn der adaptive Modus aktiviert ist, wird für den Datenverkehr eine Zulassungsregel erstellt.

Es kann vorkommen, dass der abgefangene Datenverkehr mehr als eine Regel erfüllt. In diesem Fall sorgt die Vorrangfunktion dafür, dass die Host Intrusion Prevention nur die erste in der Liste erfüllte Regel anwendet.

Ordnen der Firewall-Regelliste

Wenn Sie eine Firewall-Regelrichtlinie erstellen oder anpassen, sollten Sie die spezifischeren Regeln an den Anfang der Liste stellen und die allgemeineren Regeln ans Ende. So stellen Sie sicher, dass der Datenverkehr durch die Host Intrusion Prevention entsprechend gefiltert wird und dass keine Regeln ausgelassen werden, die auf Ausnahmen von anderen, allgemeineren Regeln basieren.

Um beispielsweise alle HTTP-Anfragen mit Ausnahme der von der IP-Adresse 10.10.10.1 stammenden zu blockieren, müssen Sie zwei Regeln erstellen:

- **Erlauben-Regel:** HTTP-Datenverkehr von Adresse 10.10.10.1 zulassen. Dies ist die spezifischste Regel.
- **Blockierregel:** Allen Datenverkehr blockieren, der den HTTP-Dienst verwendet. Diese Regel ist allgemeiner.

Sie müssen die spezifischere Zulassungsregel in der Firewall-Regelliste vor der allgemeineren Blockierregel platzieren. Damit stellen Sie sicher, dass die Firewall, wenn Sie eine HTTP-Anfrage von der Adresse 10.10.10.1 abfängt, zuerst feststellt, dass diese mit einer Regel übereinstimmt, die diesem Datenverkehr das Passieren der Firewall erlaubt.

Wenn Sie die allgemeinere Blockierregel vor der spezifischeren Zulassungsregel platzieren, dann erkennt die Host Intrusion Prevention, ob die HTTP-Anfrage von 10.10.10.1 mit der Blockierregel übereinstimmt, bevor die Ausnahme gefunden wird. Der Datenverkehr wird dann blockiert, obwohl Sie HTTP-Anfragen von dieser Adresse zulassen wollen.

Funktionsweise der statusbehafteten Filterung

Die statusbehaftete Filterung beinhaltet die Verarbeitung eines Pakets anhand von zwei Regelsätzen, einem konfigurierbaren Firewall-Regelsatz und einem dynamischen Firewall-Regelsatz oder einer Statustabelle.

Die konfigurierbaren Regeln ermöglichen zwei Arten von Aktionen:

- **Erlauben:** Das Paket wird erlaubt, und es wird ein Eintrag in der Statustabelle vorgenommen.
- **Blockieren:** Das Paket wird blockiert, und es wird kein Eintrag in der Statustabelle vorgenommen.

Die Einträge der Statustabelle stammen aus der Netzwerkaktivität und spiegeln den Status des Netzwerkstapels wider. Jede Regel in der Statustabelle hat nur eine Aktion: **Erlauben**, sodass jedes beliebige Paket, das einer Regel in der Statustabelle entspricht, automatisch erlaubt wird.

Der Filterprozess umfasst die folgenden Schritte:

1. Die Firewall vergleicht ein eingehendes Paket mit den Einträgen in der Statustabelle. Wenn das Paket einem beliebigen Eintrag in der Tabelle entspricht, wird es sofort erlaubt. Wenn nicht, wird die Liste der konfigurierbaren Firewall-Regeln überprüft.

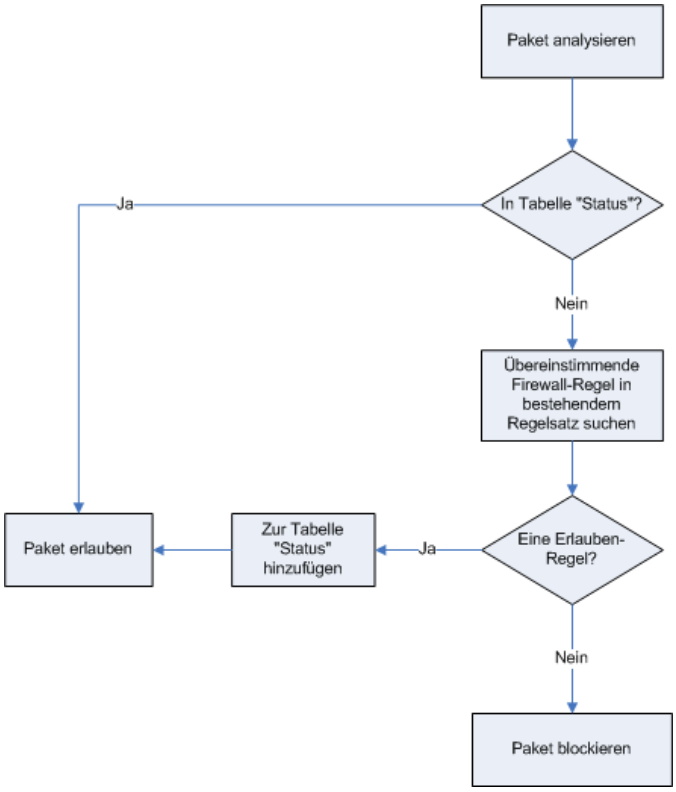
   Ein Eintrag in der Statustabelle wird als Übereinstimmung angesehen, wenn das Protokoll, die lokale Adresse, der lokale Port, die Remote-Adresse und der Remote-Port denen des Pakets entsprechen.

2. Wenn das Paket einer Erlauben-Regel entspricht, wird es erlaubt und ein Eintrag in der Statustabelle erstellt.

3 Wenn das Paket mit einer Blockierregel übereinstimmt, wird es blockiert.

4 Wenn das Paket mit keiner konfigurierbaren Regel übereinstimmt, wird es blockiert.

Abbildung 5-2 Statusbehafteter Filterprozess



Funktionsweise der statusbehafteten Paketinspizierung

Die statusbehaftete Paketinspizierung kombiniert die statusbehaftete Filterung mit dem Zugriff auf Befehle auf der Anwendungsebene, der Sicherung von Protokollen, wie FTP, DHCP und DNS.

FTP umfasst zwei Verbindungen: *Steuerung* für Befehle und *Daten* für die Information. Wenn ein Client eine Verbindung zu einem FTP-Server herstellt, wird der Steuerungskanal eingerichtet, der am FTP-Zielport 21 eingeht, und es wird ein Eintrag in der Statustabelle vorgenommen. Wenn die Firewall auf eine Verbindung stößt, die auf Port 21 geöffnet ist, führt sie eine statusbehaftete Paketinspizierung auf den Paketen durch, die über den FTP-Steuerungskanal eingehen, wenn die Option für die FTP-Inspizierung mit der Richtlinie „Firewall-Optionen“ festgelegt wurde.

Wenn der Steuerungskanal geöffnet ist, kommuniziert der Client mit dem FTP-Server. Die Firewall parsed den Befehl PORT in dem Paket, das über die Verbindung gesendet wurde, und erstellt einen zweiten Eintrag in der Statustabelle, um die Datenverbindung zu erlauben.

Wenn sich der FTP-Server im aktiven Modus befindet, öffnet der Server die Datenverbindung. Im passiven Modus initiiert der Client die Verbindung. Wenn der Server den ersten Datenübertragungsbefehl (LIST) empfängt, öffnet er die Datenverbindung in Richtung des Clients und überträgt die Daten. Der Datenkanal wird geschlossen, nachdem die Übertragung abgeschlossen ist.

Die Kombination aus Steuerungsverbindung und einer oder mehreren Datenverbindungen nennt man Sitzung, und die dynamischen FTP-Regeln werden gelegentlich als Sitzungsregeln bezeichnet. Die Sitzung wird aufrechterhalten, bis der Steuerungskanaleintrag aus der Statustabelle gelöscht wird. Während der regelmäßigen Säuberung der Tabelle werden alle Datenverbindungen nacheinander gelöscht, wenn der Steuerungskanal einer Sitzung gelöscht wurde.

Statusbehaftete Protokollverfolgung

Im Folgenden finden Sie eine Zusammenfassung der Verbindungstypen, die die statusbehaftete Firewall überwacht, und deren Verarbeitungsweise.

Protokoll	Beschreibung der Verarbeitung
UDP	Eine UDP-Verbindung wird der Statustabelle hinzugefügt, wenn eine übereinstimmende statische Regel gefunden wird und die Aktion für die Regel „Erlauben“ lautet. Generische UDP-Verbindungen, die Protokolle auf der Anwendungsebene befördern, die der Firewall unbekannt sind, verbleiben in der Statustabelle, sofern die Verbindung nicht länger im Ruhezustand ist als der angegebene Zeitraum für das Timeout.
ICMP	Nur die Nachrichtentypen „ICMP Echo Request“ und „Echo Reply“ werden nachverfolgt. Andere ICMP-Verbindungen werden wie generische UDP-Verbindungen verwaltet. **Hinweis:** Im Gegensatz zum verlässlichen, verbindungsorientierten TCP-Protokoll sind UDP und ICMP weniger verlässliche, verbindungslose Protokolle. Um diese Protokolle zu sichern, sieht die Firewall generische UDP- und ICMP-Verbindungen als virtuelle Verbindungen an, die nur so lange gehalten werden, bis die Verbindung länger im Ruhezustand ist als der Zeitraum, der für das Timeout für diese Verbindung angegeben wurde. Das Timeout für virtuelle Verbindungen wird mit der Richtlinie „Firewall-Optionen“ festgelegt.
TCP	TCP-Protokolle arbeiten mit dem „3-way Handshake“. Wenn ein Client-Computer eine neue Verbindung initiiert, sendet er ein Paket an das Ziel mit einem festgelegten SYN-Bit, was auf eine neue Verbindung hinweist. Das Ziel antwortet, indem es ein Paket an den Client mit einem SYN-ACK-Bit sendet. Der Client antwortet dann, indem er ein Paket mit einem festgelegten ACK-Bit sendet, und die statusbehaftete Verbindung wird eingerichtet. Alle ausgehenden Pakete werden erlaubt, aber nur die eingehenden Pakete, die Teil der eingerichteten Verbindung sind, werden erlaubt. Als Ausnahme bezeichnet man, wenn die Firewall erst das TCP-Protokoll abfragt und alle zuvor bestehenden Verbindungen hinzufügt, die mit den statischen Regeln übereinstimmen. Zuvor bestehende Verbindungen ohne eine damit übereinstimmende statische Regel werden blockiert. Das TCP-Verbindungstimeout, das mit der Richtlinie „Firewall-Optionen“ festgelegt wird, wird nur erzwungen, wenn die Verbindung nicht eingerichtet ist. Ein zweites oder erzwungenes TCP-Timeout gilt nur für eingerichtete TCP-Verbindungen. Dieses Timeout wird durch eine Registrierungseinstellung gesteuert und hat den Standardwert von einer Stunde. Alle vier Minuten fragt die Firewall den TCP-Stapel ab und schließt Verbindungen aus, die nicht durch TCP gemeldet werden.
DNS	Es wird eine Anforderungs-/Antwort-Übereinstimmung durchgeführt, um sicherzustellen, dass DNS-Antworten nur für den lokalen Port erlaubt werden, der die Anforderung initiiert hat, und nur von einer Remote-IP-Adresse aus, die innerhalb des virtuellen UDP-Verbindungstimeout-Intervalls abgefragt wurde. Eingehende DNS-Antworten werden unter folgenden Bedingungen erlaubt: ■ Die Verbindung in der Statustabelle ist nicht abgelaufen. ■ Die Antwort stammt von derselben Remote-IP-Adresse und dem Port, von dem aus die Anforderung geschickt wurde.

Protokoll	Beschreibung der Verarbeitung
DHCP	Es wird eine Anforderungs-Antwort-Übereinstimmung durchgeführt, um sicherzustellen, dass die ausgegebenen Pakete nur für legitime Anforderungen erlaubt werden. Dennoch werden eingehende DHCP-Antworten unter folgenden Bedingungen erlaubt: ■ Die Verbindung in der Statustabelle ist nicht abgelaufen. ■ Die Transaktions-ID für die Antwort entspricht derjenigen aus der Anforderung.
FTP	■ Die Firewall führt die statusbehaftete Paketinspizierung auf TCP-Verbindungen durch, die auf Port 21 geöffnet wurden. Die Inspizierung findet nur im Steuerungskanal statt, der ersten Verbindung, die auf diesem Port geöffnet wurde. ■ Die FTP-Inspizierung findet nur für die Pakete statt, die die neuen Informationen beinhalten. Erneut übertragene Pakete werden ignoriert. ■ Dynamische Regeln werden in Abhängigkeit von der Richtung (Client/Server) und des Modus (aktiv/passiv) erstellt: – Aktiver Client-FTP-Modus: Die Firewall erstellt eine dynamische Regel für eingehenden Verkehr, nachdem der Befehl für den Eingangsport geparsed wurde, vorausgesetzt, der Port ist mit dem Befehl RFC 959 konform. Die Regel wird gelöscht, wenn der Server die Datenverbindung initiiert oder wenn die Regel abläuft. – Aktiver Server-FTP-Modus: Die Firewall erstellt eine dynamische Regel für ausgehenden Verkehr, nachdem der Befehl für den Eingangsport geparsed wurde. – Passiver Client-FTP-Modus: Die Firewall erstellt eine dynamische Regel für ausgehenden Verkehr, wenn sie die Antwort auf den PASV-Befehl liest, die vom FTP-Server gesendet wurde, vorausgesetzt, sie kennt den PASV-Befehl vom FTP-Client und der PASV-Befehl ist mit RFC 959 konform. Die Regel wird gelöscht, wenn der Client die Datenverbindung initiiert oder wenn die Regel abläuft. – Passiver Server-FTP-Modus: Die Firewall erstellt eine dynamische Regel für eingehenden Verkehr.

Firewall-Regelgruppen und Verbindungsgruppen

Sie können Regeln für die einfachere Verwaltung gruppieren. Normale Regelgruppen haben keine Auswirkung auf die Art und Weise, wie die Host Intrusion Prevention die darin enthaltenen Regeln behandelt, diese werden auch hier von oben nach unten abgearbeitet.

Die Host Intrusion Prevention unterstützt aber auch einen Regelgruppentyp, der sich auf die Behandlung der Regeln auswirkt. Diese Gruppen werden als *Verbindungsgruppen* bezeichnet. In Verbindungsgruppen enthaltene Regeln werden nur dann verarbeitet, wenn bestimmte Kriterien erfüllt sind.

Mit Verbindungsgruppen können Sie Regeln verwalten, die nur gelten, wenn Sie eine Verbindung zu einem Netzwerk herstellen und dabei eine Kabelverbindung, eine kabellose oder eine nicht spezifische Verbindung mit bestimmten Parametern verwenden. Darüber hinaus berücksichtigen diese Gruppen den Netzwerkadapter, sodass Computer mit mehreren Netzwerkschnittstellen Regeln anwenden können, die adapterspezifisch sind. Die Parameter für erlaubte Verbindungen können einen beliebigen oder alle der folgenden Elemente für jeden Netzwerkadapter verwenden:

- IP-Adresse
- DNS-Suffix

- Gateway-IP-/MAC-Paar
- DHCP-IP-/MAC-Paar
- DNS-Server, der für das Auflösen von URLs abgefragt wurde
- verwendeter WINS-Server

Wenn zwei Verbindungsgruppen für eine Verbindung zutreffen, verwendet Host Intrusion Prevention den normalen Vorrang und verarbeitet die erste zutreffende Verbindungsgruppe in der Regelliste. Wenn keine Regel in der ersten Verbindungsgruppe übereinstimmt, wird die Regelverarbeitung fortgesetzt, und es kann eine Übereinstimmung mit einer Regel in der nächsten Gruppe vorliegen.

Wenn die Host Intrusion Prevention die Parameter einer Verbindungsgruppe mit einer aktiven Verbindung abgleicht, wendet sie die in der Verbindungsgruppe enthaltenen Kriterien an. Die Regeln werden als kleine Regelmenge behandelt und der normale Vorrang eingehalten. Wenn der abgefangene Datenverkehr einige Regeln nicht erfüllt, werden diese von der Firewall ignoriert.

Eine Verbindung wird erlaubt, wenn *alle* der folgenden Bedingungen für einen Netzwerkadapter gelten:

- Wenn der Verbindungstyp **LAN** ist.

  oder

  Wenn der Verbindungstyp **Kabellos (802.11)** ist.

  oder

  Wenn der Verbindungstyp **Alle** ist und die DNS-Suffix-Liste oder die IP-Adressliste ausgefüllt werden.

- Wenn **IP-Adressliste** ausgewählt ist, muss die IP-Adresse des Adapters mit einem der Einträge in der Liste übereinstimmen.
- Wenn **DNS-Suffix-Liste prüfen** ausgewählt ist, muss das DNS-Suffix des Adapters mit einem der Einträge in der Liste übereinstimmen. (Bei der DNS-Namensübereinstimmung wird die Groß- und Kleinschreibung beachtet.)
- Wenn **Standard-Gateway-Liste prüfen** ausgewählt ist, muss das standardmäßige Adapter-Gateway IP-/MAC-Paar mit mindestens einem der Listeneinträge übereinstimmen.
- Wenn **DHCP-Server-Liste prüfen** ausgewählt ist, muss das Adapter-DHCP IP-/MAC-Paar mit mindestens einem der Listeneinträge übereinstimmen. **Hinweis:** Die MAC-Adresse ist optional und wird nur verwendet, wenn sie angegeben ist.
- Wenn **Primäre DNS-Serverliste prüfen** ausgewählt ist, muss die Adapter-DNS-Server-IP-Adresse mit einem beliebigen der Listeneinträge übereinstimmen.
- Wenn **Sekundäre DNS-Serverliste prüfen Liste** ausgewählt ist, muss die Adapter-DNS-Server-IP-Adresse mit einem beliebigen der Listeneinträge übereinstimmen.

- Wenn **Primäre WINS-Server-Liste prüfen** ausgewählt ist, muss die primäre Adapter-WINS-Server-IP-Adresse mit mindestens einem der Listeneinträge übereinstimmen.
- If Wenn **Sekundäre WINS-Server-Liste prüfen** ausgewählt ist, muss die sekundäre Adapter-WINS-Server-IP-Adresse mit mindestens einem der Listeneinträge übereinstimmen.

Firewall – Lernmodus und adaptiver Modus

Wenn Sie die Firewall-Funktion aktivieren, überwacht die Host Intrusion Prevention kontinuierlich den von einem Computer gesendeten und darauf empfangenen Netzwerkdatenverkehr. Auf der Grundlage der Firewall-Regelrichtlinie kann Datenverkehr zugelassen oder blockiert werden. Wenn der Datenverkehr keiner Regel entspricht, wird er automatisch blockiert – sofern der Lernmodus oder der adaptive Modus der Firewall aktiviert ist.

Den Lernmodus können Sie nur für die eingehende Kommunikation, nur für die ausgehende Kommunikation oder für beide Richtungen aktivieren.

Im Lernmodus zeigt Host Intrusion Prevention eine Lernmodus-Warnung an, wenn unbekannter Netzwerkverkehr abgefangen wird. In diesem Dialogfeld wird der Benutzer aufgefordert, Datenverkehr, der keiner der vorhandenen Regeln entspricht, zuzulassen oder zu blockieren. Dabei werden automatisch dynamische Regeln für nicht übereinstimmenden Datenverkehr erstellt.

Im adaptiven Modus erstellt die Host Intrusion Prevention automatisch eine Zulassungsregel, die jeden Datenverkehr zulässt, der mit keiner der vorhandenen Blockierregeln übereinstimmt. Dabei werden automatisch dynamische Zulassungsregeln für nicht übereinstimmenden Datenverkehr erstellt.

Aus Sicherheitsgründen werden jedoch in beiden Modi (Lernmodus und adaptiver Modus) eingehende Pings blockiert, sofern nicht eine explizite Zulassungsregel für eingehenden ICMP-Datenverkehr erstellt wird. Außerdem wird eingehender Datenverkehr an einem Port, der auf dem Host nicht geöffnet ist, blockiert, sofern nicht für den Datenverkehr eine explizite Zulassungsregel erstellt wird. Beispiel: Wenn der Telnet-Dienst auf dem Host nicht gestartet ist, dann wird eingehender TCP-Datenverkehr an Port 23 (Telnet) auch dann blockiert, wenn keine explizite Regel vorliegt, die diesen Datenverkehr blockiert. Sie können für jeden erwünschten Datenverkehr eine explizite Zulassungsregel erstellen.

Die Host Intrusion Prevention zeigt alle Regeln an, die im Lernmodus oder im adaptiven Modus auf Clients erstellt wurden, und ermöglicht das Speichern und Migrieren dieser Regeln in Administratorregeln.

Statusbehaftete Filterung

Wenn der adaptive oder der Lernmodus mit der statusbehafteten Firewall angewendet wird, ändert sich der Filterprozess etwas, um die adaptive Erstellung einer neuen Regel zu erlauben, damit das eingehende Paket verarbeitet werden kann. Dieser Filterprozess fährt wie folgt fort:

1. Die Firewall vergleicht ein eingehendes Paket mit den Einträgen in der Statustabelle und findet keine Übereinstimmung. Anschließend überprüft die Firewall die Liste mit statischen Regeln und findet keine Übereinstimmung.
2. Es wird kein Eintrag in der Statustabelle vorgenommen, aber falls es sich um ein TCP-Paket handelt, wird es in eine Liste ausstehender Elemente aufgenommen. Wenn nicht, wird das Paket entfernt.

3 Wenn neue Regeln erlaubt werden, wird eine unidirektionale statische Erlauben-Regel erstellt. Wenn es sich um ein TCP-Paket handelt, wird ein Eintrag in der Statustabelle vorgenommen.

4 Wenn eine neue Regel nicht erlaubt wird, wird das Paket verweigert.

Quarantäne-Richtlinien und -Regeln

Wenn ein Client nach längerer Abwesenheit in das Netzwerk zurückkehrt, schränken die Quarantänerichtlinien seine Kommunikationsmöglichkeiten mit dem Netzwerk ein, bis der ePolicy Orchestrator überprüft hat, dass der Client alle neuen Richtlinien, Software-Updates und DAT-Dateien besitzt.

Die Host Intrusion Prevention setzt die Quarantäneregeln für *alle* von ePolicy Orchestrator verwalteten Anwendungen durch. Wenn Sie daher Clients mit VirusScan Enterprise mithilfe von ePolicy Orchestrator verwalten, isoliert die Host Intrusion Prevention alle in das Netzwerk zurückkehrenden Clients, auf denen die Ausführung von VirusScan Enterprise-Tasks fehlschlägt. Dies ist z. B. der Fall, wenn eine Update-Task die neuesten DAT-Dateien nicht abrufen kann.

Veraltete Richtlinien und Dateien können Sicherheitslücken verursachen und Systeme für Angriffe verletzbar machen. Indem Benutzer bis zur Aktualisierung durch ePolicy Orchestrator isoliert bleiben, werden unnötige Sicherheitsrisiken vermieden. Beispielsweise ist eine Quarantänerichtlinie nützlich für Notebooks, deren Richtlinien und Dateien möglicherweise veralten, wenn sie sich mehrere Tage außerhalb des Firmennetzwerkes befinden.

Wenn Sie die Quarantänerichtlinie aktivieren, arbeiten ePolicy Orchestrator und die Host Intrusion Prevention zusammen. ePolicy Orchestrator erkennt, ob ein Benutzer die erforderlichen aktuellsten Informationen besitzt. Die Host Intrusion Prevention setzt die Isolierung des Clients bis zur Aktualisierung der notwendigen Richtlinien und Dateien durch.

Wenn sich ein Benutzer mittels VPN-Software mit Ihrem Netzwerk verbindet, dann sollten Sie sicherstellen, dass die Quarantäneregeln den Datenverkehr zulassen, der für die Verbindung und die Authentifizierung über VPN erforderlich ist.

Beim Konfigurieren der Richtlinie für Quarantäneoptionen geben Sie eine Liste isolierter IP-Adressen und Subnetze an. Alle einer dieser Adressen zugewiesenen Benutzer werden durch die Host Intrusion Prevention bei der Rückkehr in das Netzwerk isoliert.

Wenn eine Richtlinie für Quarantäneoptionen auf einen Client angewendet wird, verwendet die Host Intrusion Prevention den ePolicy Orchestrator-Agenten, um herauszufinden, ob der Client die aktuellsten Richtlinien und Dateien besitzt. Dabei wird auch geprüft, ob alle ePolicy Orchestrator-Tasks korrekt ausgeführt wurden.

Wenn der Benutzer auf dem aktuellen Stand ist, hebt die Host Intrusion Prevention die Isolierung des Clients sofort auf.

Wenn mindestens eine ePolicy Orchestrator-Task nicht ausgeführt wurde, besitzt der Benutzer jedoch keine aktuellen Daten, und die Host Intrusion Prevention hebt die Isolierung des Clients nicht automatisch auf. Der Client bleibt dann gegebenenfalls für einige Minuten isoliert, während der ePolicy Orchestrator-Agent die Richtlinien und Dateien aktualisiert. Host Intrusion Prevention kann die Isolierung fortsetzen oder anhalten – dies wird durch die Einstellungen in der Richtlinie für die Quarantäne-optionen festgelegt. Wenn Sie die Host Intrusion Prevention so konfigurieren, dass die Quarantäne weiterhin durchgesetzt wird, kann es passieren, dass Clients über einen längeren Zeitraum isoliert bleiben.

Mit der Quarantänerichtlinie setzt die Host Intrusion Prevention einen strikten Satz von Firewall-Quarantäneregeln durch, die festlegen, mit wem isolierte Clients kommunizieren dürfen.

Für den Quarantänemodus muss die Firewall aktiviert sein. Die Aktivierung des Quarantänemodus findet nur statt, wenn auch die Firewall aktiviert ist.

Migration von benutzerdefinierten 6.0-Firewall-Regeln zu 6.1-Regeln

Verwenden Sie das Host Intrusion Prevention-Dienstprogramm zur Migration von Firewall-Regeln, um benutzerdefinierte 6.0-Firewall-Regelrichtlinien zu den entsprechenden 6.1-Richtlinien zu migrieren. Die migrierten Richtlinien erscheinen unter Firewall-Regeln oder Quarantäneregeln mit dem Text **[Migriert]** vor dem Namen der Richtlinie. Sie werden automatisch denselben Clients zugewiesen wie die entsprechenden 6.0-Richtlinien.

Sie können 6.0-Firewall-Regeln mit einer von zwei Methoden migrieren:

- *Übersetzen* ändert die Regeln, um die statusbehaftete Firewall-Funktionalität zu nutzen.
- *Kopieren* kopiert, ohne die Regeln zu verändern.

Bei beiden Methoden werden die migrierten Firewall-Regelrichtlinien automatisch denselben Clients zugewiesen wie die entsprechenden 6.0-Richtlinien.

Clients der Version 6.0 erkennen nur Richtlinien für 6.0-Firewall-Regeln und 6.0-Quarantäneregeln, und Clients der Version 6.1 erkennen nur Richtlinien für Firewall-Regeln und Quarantäneregeln.

So migrieren Sie Regeln:

1. Doppelklicken Sie auf den Link für das Migrationsdienstprogramm im installierten McAfee ePO-Ordner (`C:\Programme\McAfee\ePO\3.6.x\Host HIPS Firewall Rule Migrator`).
2. Geben Sie den Benutzernamen und das Passwort eines globalen ePO-Administrators ein, und klicken Sie auf **Anmelden**.
3. Wählen Sie die Migrationsmethode, **Übersetzen** oder **Kopieren**, und klicken Sie auf **Migrieren**.
4. Prüfen Sie nach Abschluss der Migration die Liste der neuen Richtlinien unter **Firewall-Regeln** und **Quarantäneregeln**, und benennen Sie Regeln um, oder weisen Sie sie neu zu, wie erforderlich.

Vordefinierte Firewall-Richtlinien

Die Firewall-Funktion in der Host Intrusion Prevention enthält vier Richtlinienkategorien:

- **Firewall-Optionen:** Aktiviert bzw. deaktiviert den Firewall-Schutz. Die vordefinierten Richtlinien umfassen **Aus (McAfee-Standard)**, **Ein**, **Adaptiv, Lernmodus**.
- **6.0-Firewall-Regeln** (nur 6.0 Clients): Legt die Firewall-Regeln fest. Die vordefinierten Richtlinien umfassen **Minimal (McAfee-Standard)**, **Lernender Beginner**, **Client Hoch**, **Client Mittel**, **Server Hoch**, **Server Mittel**.
- **Firewall-Regeln** (nur 6.1 Clients): Legt die Firewall-Regeln fest. Die vordefinierten Richtlinien umfassen **Minimal (McAfee-Standard)**, **Lernender Beginner**, **Client Hoch**, **Client Mittel**, **Server Hoch**, **Server Mittel**.
- **Quarantäneoptionen:** Aktiviert bzw. deaktiviert den Quarantänemodus. Die vordefinierte Richtlinie ist **Deaktiviert (McAfee-Standard)**.
- **6.0-Quarantäneregeln** (nur 6.0 Clients): Legt die während der Quarantäne angewendeten Firewall-Regeln fest. Die vordefinierte Richtlinie ist die Standardrichtlinie **(McAfee-Standard)**.
- **Quarantäneregeln** (nur 6.1 Clients): Legt die während der Quarantäne angewendeten Firewall-Regeln fest. Die vordefinierte Richtlinie ist die Standardrichtlinie **(McAfee-Standard)**.

Direktzugriff

Die Firewall-Funktion bietet Verknüpfungen (*) für den Direktzugriff zur Überwachung und Verwaltung von Firewall-Regeln und Firewall-Client-Regeln.

Abbildung 5-3 Firewall-Funktion

Konfigurieren der Richtlinie für Firewall-Optionen

Mithilfe der Richtlinie für die Firewall-Optionen können Sie die Firewall aktivieren bzw. deaktivieren und für Clients den adaptiven Modus oder den Lernmodus anwenden. Sie können aus vier vorkonfigurierten Richtlinien auswählen oder eine neue Richtlinie erstellen und anwenden.

So konfigurieren Sie die Richtlinie für Firewall-Optionen:

1 Wählen Sie in der Konsolenstruktur die Gruppe oder den Computer aus, auf den die Richtlinie angewendet werden soll.

2 Erweitern Sie auf der Registerkarte **Richtlinien** die Funktion **Host Intrusion Prevention-Firewall**.

3 Klicken Sie in der Zeile **Firewall-Optionen** auf **Bearbeiten**.

Die Liste der Richtliniennamen wird aktiviert.

4 Führen Sie einen der folgenden Vorgänge aus:

- Wählen Sie in der Liste eine vorkonfigurierte Richtlinie aus, und klicken Sie auf **Anwenden**:

Wählen Sie...	Für folgende Einstellungen...
Aus (McAfee-Standard)	Alle deaktiviert
Ein	■ Firewall aktivieren ■ Regulären Schutz aktivieren ■ Client-Ausnahmen speichern
Adaptiv	■ Firewall aktivieren ■ Adaptiven Modus aktivieren ■ Client-Ausnahmen speichern
Lernen	■ Firewall aktivieren ■ Lernmodus aktivieren, eingehend und ausgehend ■ Client-Ausnahmen speichern

- Wählen Sie **Neue Richtlinie**.

  Das Dialogfeld **Neue Richtlinie erstellen** wird geöffnet.

Sie können eine neue duplizierte Richtlinie erstellen, wenn Sie die Einzelheiten zu einer vordefinierten Richtlinie anzeigen, indem Sie unten im Dialogfeld für die Richtlinie auf **Duplizieren** klicken. Geben Sie den Namen der neuen Richtlinie ein, und geben Sie an, ob die Richtlinie augenblicklich dem aktuellen Knoten zugewiesen werden soll.

5 Wählen Sie die Richtlinie aus, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein, und klicken Sie auf **OK**.

Das Dialogfeld **Firewall-Optionen** wird geöffnet.

Abbildung 5-4 Firewall-Optionen

6 Wählen Sie die entsprechenden Einstellungen. Klicken Sie auf **Hilfe**, um Details nachzuschlagen.

7 Klicken Sie auf **Anwenden**, und schließen Sie das Dialogfeld.

Der Name der neuen Richtlinie wird in der Richtlinienliste angezeigt.

8 Klicken Sie auf **Übernehmen**.

Konfigurieren der Richtlinie für Firewall-Regeln

Firewall-Regeln legen fest, wie ein System beim Abfangen von Netzwerkdatenverkehr arbeitet, indem der Datenverkehr entweder zugelassen oder blockiert wird. Das Erstellen und Verwalten von Firewall-Regeln realisieren Sie, indem Sie eine Richtlinie **Firewall-Regeln** mit den entsprechenden Einstellungen anwenden.

Die Richtlinie für **Firewall-Regeln** bietet Zugriff auf:

- *Erstellen neuer Richtlinien für Firewall-Regeln*
- *Anzeigen und Bearbeiten von Firewall-Regeln*
- *Erstellen einer neuen Firewall-Regel oder Firewall-Gruppe*
- *Löschen einer Firewall-Regel oder -Gruppe*
- *Anzeigen von Firewall-Client-Regeln*

Erstellen neuer Richtlinien für Firewall-Regeln

Um eine neue, nicht knotenspezifische Richtlinie hinzuzufügen, müssen Sie die Richtlinie im **Richtlinienkatalog** erstellen. Nähere Informationen dazu finden Sie unter *Richtlinienkatalog* auf Seite 128. Um eine neue knotenspezifische Richtlinie hinzuzufügen, müssen Sie die in diesem Abschnitt beschriebenen Schritte durchführen.

So erstellen Sie eine neue Richtlinie für Firewall-Regeln:

1. Wählen Sie in der Konsolenstruktur die Gruppe oder den Computer aus, auf den die Richtlinie angewendet werden soll.
2. Erweitern Sie auf der Registerkarte „Richtlinien“ die Funktion „Firewall“.
3. Klicken Sie in der Zeile **Firewall-Regeln** auf **Bearbeiten**.

   Die Liste der Richtliniennamen wird aktiviert.
4. Führen Sie einen der folgenden Vorgänge aus:

   - Wählen Sie in der Liste eine der vorkonfigurierten Richtlinien aus, und klicken Sie auf **Anwenden**.

Wählen Sie folgende Richtlinie...	Für folgenden Schutz...
Minimal (Standard)	■ Blockiert den gesamten eingehenden ICMP-Datenverkehr, der von einem Angreifer verwendet werden kann, um Informationen über Ihren Computer zu sammeln. Den übrigen ICMP-Datenverkehr lässt die Host Intrusion Prevention zu. ■ Erlaubt Windows-Dateifreigabeanfragen von Computern im selben Subnetz. Von anderen Computern stammende Anfragen werden blockiert. (Bei der Richtlinie „Vertrauenswürdige Netzwerke“ muss **Lokales Subnetz automatisch einschließen** ausgewählt sein.) ■ Erlaubt das Durchsuchen von Windows-Domänen, Arbeitsgruppen und Computern. ■ Erlaubt den gesamten über hohe Ports eingehenden und ausgehenden UDP-Datenverkehr. ■ Erlaubt Datenverkehr, der BOOTP-, DNS- und Net Time UDP-Ports verwendet.

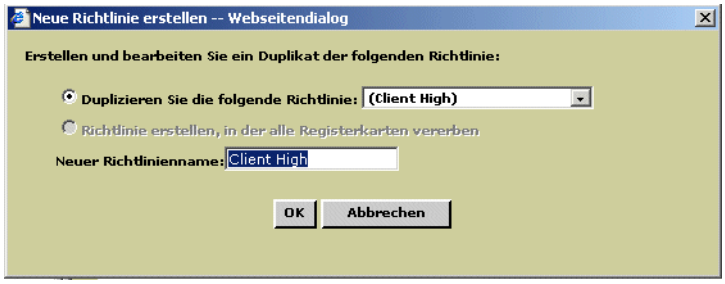
Wählen Sie folgende Richtlinie...	Für folgenden Schutz...
Lernender Beginner	■ Blockiert den eingehenden ICMP-Datenverkehr, der von einem Angreifer verwendet werden kann, um Informationen über Ihren Computer zu sammeln. Den übrigen ICMP-Datenverkehr lässt die Host Intrusion Prevention zu. ■ Erlaubt Windows-Dateifreigabeanfragen von Computern im selben Subnetz. Von anderen Computern stammende Anfragen werden blockiert. (Bei der Richtlinie „Vertrauenswürdige Netzwerke“ muss **Lokales Subnetz automatisch einschließen** ausgewählt sein.) ■ Erlaubt das Durchsuchen von Windows-Domänen, Arbeitsgruppen und Computern. ■ Erlaubt Datenverkehr, der BOOTP-, DNS- und Net Time UDP-Ports verwendet.
Client Mittel	■ Lässt nur den ICMP-Datenverkehr zu, der für IP-Netzwerkverbindungen benötigt wird (einschließlich ausgehender Pings und eingehender ICMP-Nachrichten). Der übrige ICMP-Datenverkehr wird von der Host Intrusion Prevention blockiert. ■ Lässt den für den Zugriff auf IP-Informationen notwendigen UDP-Datenverkehr zu (wie beispielsweise auf Ihre eigene IP-Adresse oder die Netzwerkzeit). Bei dieser Schutzebene wird außerdem Datenverkehr über hohe UDP-Ports (1.024 oder darüber) zugelassen. ■ Erlaubt die Windows-Dateifreigabe, allerdings nur für ein lokales Subnetz. Sie können nicht auf außerhalb Ihres lokalen Subnetzes liegende Dateien zugreifen. Durch diesen Schutz werden alle Zugriffe auf Dateien auf Ihrem Computer blockiert, die von außerhalb Ihres Subnetzes erfolgen. (Bei der Richtlinie „Vertrauenswürdige Netzwerke“ muss **Lokales Subnetz automatisch einschließen** ausgewählt sein.)
Client Hoch	Verwenden Sie diese Schutzebene, wenn Sie angegriffen werden oder wenn das Risiko eines Angriffes hoch ist. Innerhalb dieser Schutzebene wird auf Ihrem System nur ein minimaler ein- und ausgehender Datenverkehr zugelassen. ■ Lässt nur den für die Netzwerkverbindung erforderlichen ICMP-Datenverkehr zu. Dieser Schutz blockiert sowohl eingehende als auch ausgehende Pings. ■ Lässt nur den für den Zugriff auf IP-Informationen notwendigen UDP-Datenverkehr zu (wie beispielsweise auf Ihre eigene IP-Adresse oder die Netzwerkzeit). ■ Blockiert die Windows-Dateifreigabe.
Server Mittel	Verwenden Sie diese Schutzebene für einen Netzwerkserver. ■ Lässt nur den für die bessere Kommunikation zwischen Server und Clients erforderlichen ICMP-Datenverkehr zu. Der übrige ICMP-Datenverkehr wird durch diesen Schutz blockiert. ■ Lässt den für den Zugriff auf IP-Informationen erforderlichen UDP-Datenverkehr zu. Bei diesem Schutz wird außerdem Datenverkehr über hohe UDP-Ports (1.024 oder darüber) zugelassen.

Wählen Sie folgende Richtlinie...	Für folgenden Schutz...
Server Hoch	Verwenden Sie diese Schutzebene für einen Server, der direkt mit dem Internet verbunden und einem hohen Angriffsrisiko ausgesetzt ist. Verwenden Sie diese Schutzebene als Grundlage zum Erstellen Ihres eigenen Regelsatzes. ■ Lässt bestimmten ICMP-Datenverkehr zu – den Datenverkehr, der die Kommunikation zwischen dem Server und seinen Clients erleichtert. Der übrige ICMP-Datenverkehr wird von der Host Intrusion Prevention blockiert. ■ Lässt den für den Zugriff auf IP-Informationen erforderlichen UDP-Datenverkehr zu. Der übrige UDP-Datenverkehr wird von der Host Intrusion Prevention blockiert.

- Wählen Sie **Neue Richtlinie**, um eine neue Richtlinie zu erstellen.

Das Dialogfeld **Neue Richtlinie erstellen** wird geöffnet.

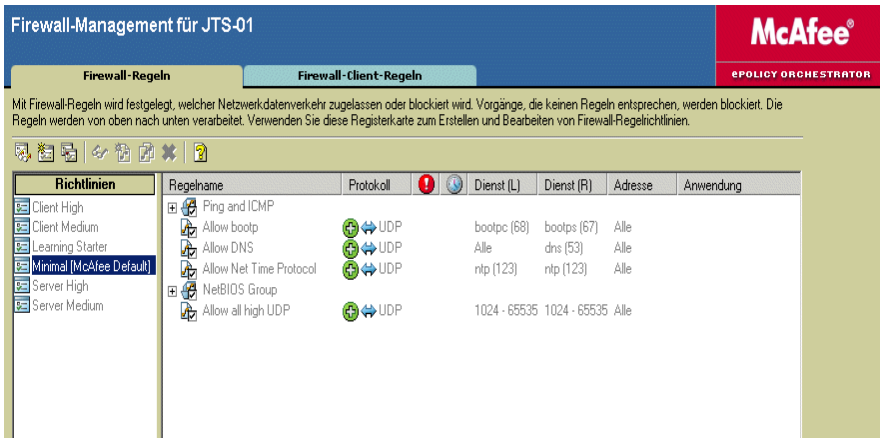
Abbildung 5-5 Dialogfeld „Neue Richtlinie erstellen“



5 Wählen Sie die Richtlinie aus, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein, und klicken Sie auf **OK**.

Das Dialogfeld **Firewall-Regeln** wird geöffnet. Die neue Richtlinie ist in der Richtlinienliste ausgewählt.

Abbildung 5-6 Registerkarte „Firewall-Regeln“



6 Führen Sie einen der folgenden Schritte aus:

- Regeln oder Gruppen hinzufügen (siehe *Erstellen einer neuen Firewall-Regel oder Firewall-Gruppe* auf Seite 91).
- Regeln bearbeiten (siehe *Anzeigen und Bearbeiten von Firewall-Regeln*).
- Regeln entfernen (siehe *Löschen einer Firewall-Regel oder -Gruppe* auf Seite 94).

7 Klicken Sie auf **Schließen**.

Der Name der neuen Richtlinie wird in der Richtlinienliste angezeigt.

8 Klicken Sie auf **Anwenden**.

Eine neue Richtlinie können Sie auch im Dialogfeld **Firewall-Regeln** erstellen, indem Sie auf **Richtlinie hinzufügen** oder auf **Richtlinie duplizieren** klicken.

Anzeigen und Bearbeiten von Firewall-Regeln

Um die Optionen zu ändern, können Sie die Details einer Regel anzeigen und bearbeiten. Dies geschieht im Dialogfeld **Firewall-Regeln** auf der Registerkarte „Firewall-Regelrichtlinien“.

So zeigen Sie eine Firewall-Regel an und bearbeiten sie:

1 Wählen Sie auf der Registerkarte **Firewall-Regeln** eine Richtlinie aus der Liste **Richtlinien** aus, und wählen Sie anschließend im Detailbereich die Regel aus, die Sie anzeigen oder bearbeiten möchten.

2 Klicken Sie im Kontextmenü bzw. in der Symbolleiste auf **Eigenschaften**.

Das Dialogfeld **Firewall-Regel** wird geöffnet.

3 Ändern Sie die Regeleinstellungen nach Ihren Vorstellungen. Klicken Sie auf **Hilfe**, um Details nachzuschlagen.

4 Klicken Sie auf **OK**, um die Änderungen zu speichern.

Erstellen einer neuen Firewall-Regel oder Firewall-Gruppe

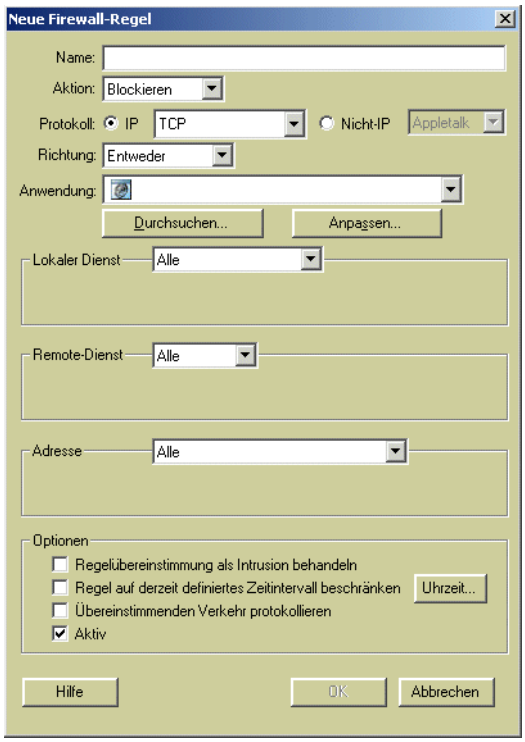
Sie können eine völlig neue Regel erstellen oder eine vorhandene Regel duplizieren und bearbeiten. Außerdem können Sie eine Gruppe für eine bestimmte Regelmenge oder eine Verbindungsgruppe erstellen sowie vordefinierte Regeln hinzufügen. Neue Regeln und Gruppen können Sie auf der Registerkarte **Firewall-Regeln** in der Firewall-Regelrichtlinie erstellen.

So erstellen Sie eine Firewall-Regel:

1 Klicken Sie auf der Registerkarte **Firewall-Regeln** in der Firewall-Regelrichtlinie auf **Hinzufügen** und anschließend auf **Neue Regel**.

Das Dialogfeld **Firewall-Regel** wird geöffnet.

Abbildung 5-7 Dialogfeld „Neue Firewall-Regel“



2 Wählen Sie die entsprechenden Einstellungen.

3 Klicken Sie auf **OK**.

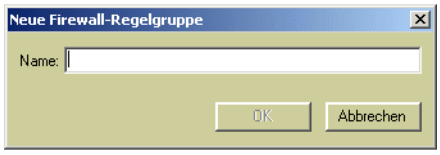
Sie können auch Regeln erstellen, indem Sie zur Richtlinie vordefinierte Regeln und Regelgruppen hinzufügen. Klicken Sie auf **Hinzufügen** und dann auf **Vordefinierte Regeln**. Wählen Sie im Dialogfeld **Vordefinierte Regeln auswählen** die Gruppe oder einzelne Regeln, die Sie hinzufügen möchten. Klicken Sie dann auf **OK**.

So erstellen Sie eine neue Regelgruppe:

1 Klicken Sie auf der Registerkarte **Firewall-Regeln** in der Firewall-Regelrichtlinie auf **Hinzufügen** und anschließend auf **Neue Gruppe**.

Das Dialogfeld **Firewall-Regelgruppe** wird geöffnet.

Abbildung 5-8 Dialogfeld „Neue Firewall-Gruppe“



2 Geben Sie im Feld **Name** einen Namen für die Gruppe ein.

3 Klicken Sie auf **OK**, um die Gruppe hinzuzufügen.

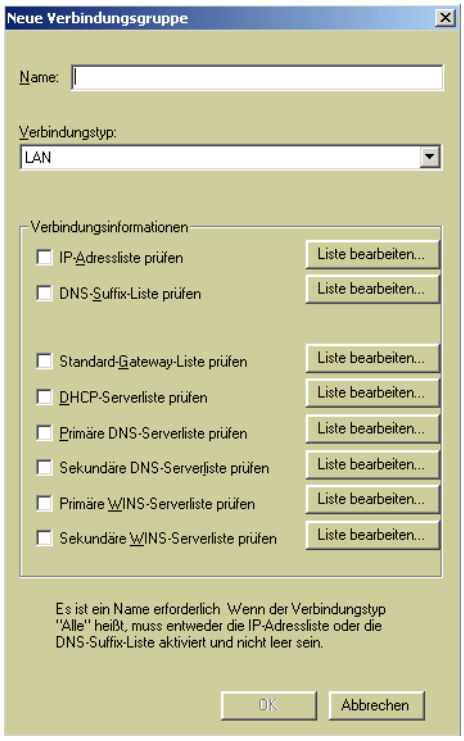
Jetzt können Sie in dieser Gruppe neue Regeln erstellen oder vorhandene Regeln aus der Firewall-Regelliste in die Gruppe verschieben.

So erstellen Sie eine Verbindungsgruppe:

1 Klicken Sie auf der Registerkarte **Firewall-Regeln** in der Firewall-Regelrichtlinie auf **Hinzufügen** und anschließend auf **Neue Verbindungsgruppe**.

Das Dialogfeld **Neue Verbindungsgruppe** wird geöffnet.

Abbildung 5-9 Dialogfeld „Neue Verbindungsgruppe“



2 Geben Sie im Feld **Name** einen Namen für die Gruppe ein.

3 Wählen Sie unter **Verbindungstyp** den Typ der Verbindung (**LAN, kabellos (802.11), alle**), für den die in dieser Gruppe enthaltenen Regeln angewendet werden sollen.

4 Wählen Sie ein Kontrollkästchen **Verbindungsinformationen** aus, um die Gruppe zu definieren, und klicken Sie anschließend auf die entsprechende Option **Liste bearbeiten**, um eine oder mehrere Adressen oder DNS-Suffixe hinzuzufügen.

- Wenn Sie **Alle** als Verbindungstyp auswählen, werden Sie aufgefordert, entweder **IP-Adressliste prüfen** oder **DNS-Suffix-Liste prüfen** auszuwählen und die entsprechende Liste zu bearbeiten.
- Geben Sie nur für DHCP-Server im selben Client-Subnetz wie der Client eine DHCP-Server-MAC-Adresse an. Identifizieren Sie DHCP-Remote-Server nur anhand ihrer IP-Adresse.

5 Klicken Sie auf **OK**.

Jetzt können Sie in dieser Gruppe neue Regeln erstellen oder vorhandene Regeln aus der Firewall-Regelliste in die Gruppe verschieben. Alle drei Verbindungsgruppen werden in der Liste mit Firewall-Regeln mit demselben Symbol angezeigt wie der in Klammern angezeigte Verbindungstyp.

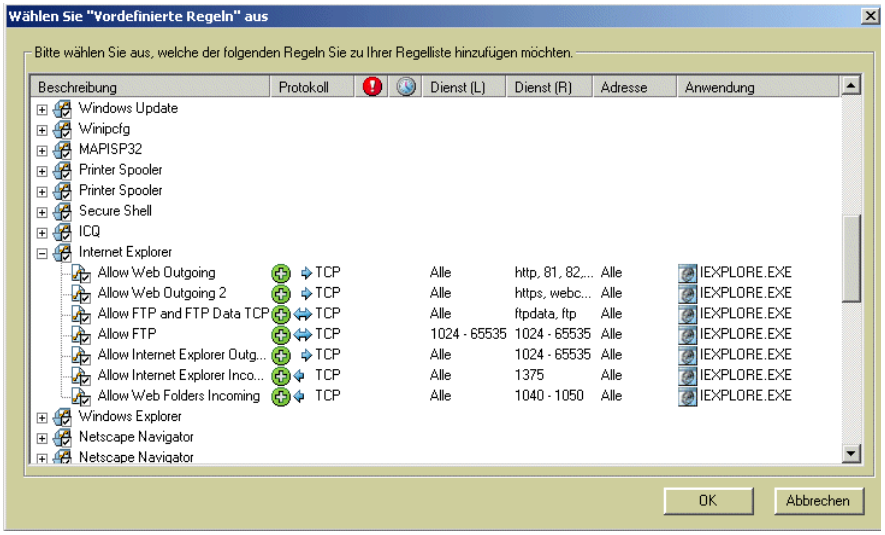
Weitere Informationen zu Verbindungsgruppen finden Sie unter *Firewall-Regelgruppen und Verbindungsgruppen* auf Seite 79.

So fügen Sie vordefinierte Regeln hinzu:

1 Klicken Sie auf der Registerkarte **Firewall-Regeln** in der Firewall-Regelrichtlinie auf **Hinzufügen** und anschließend auf **Vordefinierte Regeln**.

Das Dialogfeld **Vordefinierte Regeln auswählen** wird geöffnet.

Abbildung 5-10 Auswahl des Dialogfeldes „Vordefinierte Regeln“


Wählen Sie "Vordefinierte Regeln" aus
Bitte wählen Sie aus, welche der folgenden Regeln Sie zu Ihrer Regelliste hinzufügen möchten.
Beschreibung
Protokoll
Dienst (L)
Dienst (R)
Adresse
Anwendung
Windows Update
Winipcfg
MAPISP32
Printer Spooler
Printer Spooler
Secure Shell
ICQ
Internet Explorer
Allow Web Outgoing TCP Alle http, 81, 82,... Alle IEXPLORE.EXE
Allow Web Outgoing 2 TCP Alle https, webc... Alle IEXPLORE.EXE
Allow FTP and FTP Data TCP TCP Alle ftpdata, ftp Alle IEXPLORE.EXE
Allow FTP TCP 1024 - 65535 1024 - 65535 Alle IEXPLORE.EXE
Allow Internet Explorer Outg... TCP Alle 1024 - 65535 Alle IEXPLORE.EXE
Allow Internet Explorer Inco... TCP Alle 1375 Alle IEXPLORE.EXE
Allow Web Folders Incoming TCP Alle 1040 - 1050 Alle IEXPLORE.EXE
Windows Explorer
Netscape Navigator
Netscape Navigator
OK
Abbrechen

2 Wählen Sie eine oder mehrere Gruppen oder in einer Gruppe vorhandene Regeln aus.

3 Klicken Sie auf **OK**, um die ausgewählten Gruppen und Regeln hinzuzufügen.

Löschen einer Firewall-Regel oder -Gruppe

Regeln und Gruppen können Sie auf der Registerkarte **Firewall-Regeln** in der Firewall-Regelrichtlinie löschen.

So löschen Sie eine Firewall-Regel oder -Gruppe:

1 Wählen Sie die Registerkarte **Firewall-Regeln** in der Firewall-Regelrichtlinie aus, und wählen Sie die zu löschenden Regeln bzw. Gruppen aus.

2 Klicken Sie auf **Löschen**.

3 Klicken Sie im Bestätigungsdialogfeld auf **Ja**, um die Elemente aus der Liste zu entfernen.

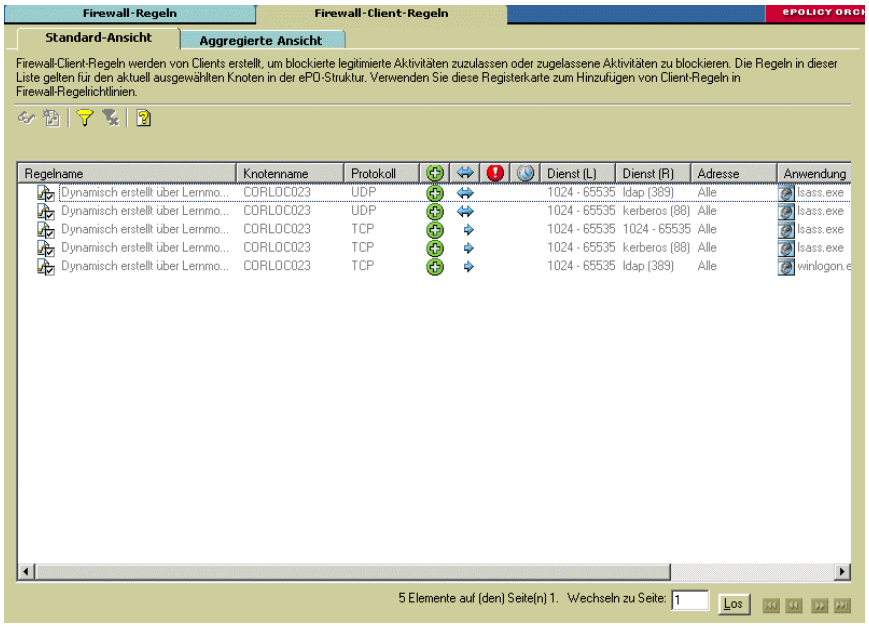
Anzeigen von Firewall-Client-Regeln

Auf der Registerkarte **Firewall-Client-Regeln** werden alle auf Client-Systemen erstellten Firewall-Regeln angezeigt. In der **Standard-Ansicht** werden alle Regeln angezeigt, auch Duplikate. In der **Aggregierten Ansicht** werden Regeln als Gruppen mit von Ihnen festgelegten ähnlichen Merkmalen angezeigt.

So zeigen Sie alle Client-Firewall-Regeln an:

1 Wählen Sie die Registerkarte **Firewall-Client-Regeln** in der Firewall-Regelrichtlinie aus, und klicken Sie auf die Registerkarte **Standard-Ansicht**.

Abbildung 5-11 Firewall-Client-Regeln – Reguläre Ansicht


Firewall-Regeln
Firewall-Client-Regeln
Standard-Ansicht
Aggregierte Ansicht
Firewall-Client-Regeln werden von Clients erstellt, um blockierte legitimierte Aktivitäten zuzulassen oder zugelassene Aktivitäten zu blockieren. Die Regeln in dieser Liste gelten für den aktuell ausgewählten Knoten in der ePO-Struktur. Verwenden Sie diese Registerkarte zum Hinzufügen von Client-Regeln in Firewall-Regelrichtlinien.
Regelname
Knotenname
Protokoll
Dienst (L)
Dienst (R)
Adresse
Anwendung
Dynamisch erstellt über Lernmo... CORLOC023 UDP 1024 - 65535 ldap (389) Alle lsass.exe
Dynamisch erstellt über Lernmo... CORLOC023 UDP 1024 - 65535 kerberos (88) Alle lsass.exe
Dynamisch erstellt über Lernmo... CORLOC023 TCP 1024 - 65535 1024 - 65535 Alle lsass.exe
Dynamisch erstellt über Lernmo... CORLOC023 TCP 1024 - 65535 kerberos (88) Alle lsass.exe
Dynamisch erstellt über Lernmo... CORLOC023 TCP 1024 - 65535 ldap (389) Alle winlogon.e
5 Elemente auf (den) Seite(n) 1. Wechseln zu Seite: 1
Los

2 Führen Sie einen der folgenden Schritte aus, um die Ansicht zu ändern:

Ziel	Aktion...
Details einer Regel anzeigen	Wählen Sie die Regel, und klicken Sie auf **Eigenschaften**.
Eine Regel zu einer Richtlinie verschieben	Wählen Sie die Regel, und klicken Sie auf **Zu Richtlinie hinzufügen**.

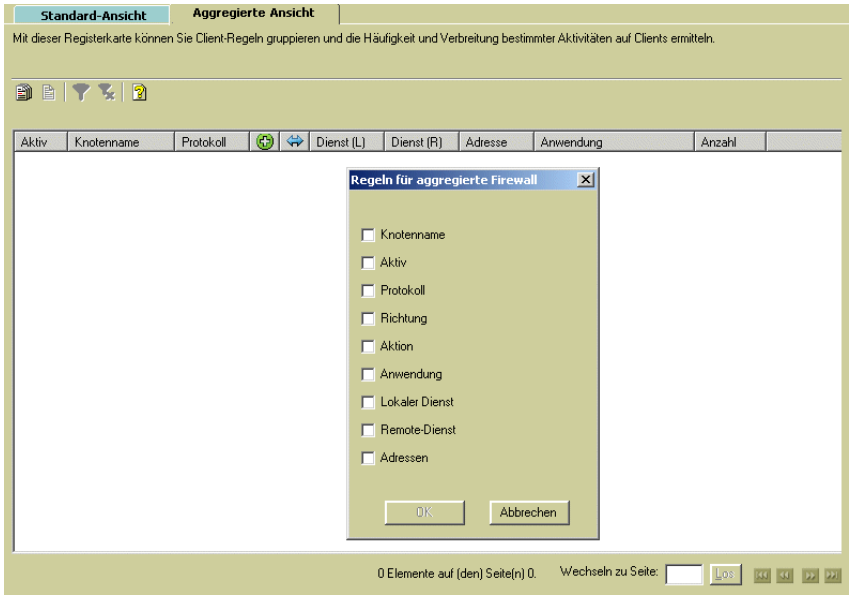
Ziel	Aktion...
Die Liste der Regeln durchblättern	Klicken Sie in der Symbolleiste auf die Navigationsschaltflächen.
Die Liste der Regeln filtern	Klicken Sie auf **Filter festlegen**. Aktivieren Sie im Dialogfeld **Anwendungsfilter festlegen** eines oder mehrere Kontrollkästchen, und geben Sie einen Wert in das entsprechende Feld ein, um einen Filter festzulegen.

So zeigen Sie aggregierte Firewall-Client-Regeln an:

1 Wählen Sie die Registerkarte **Firewall-Client-Regeln** in der Firewall-Regelrichtlinie aus, und klicken Sie auf die Registerkarte **Aggregierte Ansicht**.

Klicken Sie auf **Spalte auswählen**, damit das Dialogfeld **Aggregierte Firewall-Regel** geöffnet wird, falls es nicht bereits angezeigt wird.

Abbildung 5-12 Client-Firewall-Regeln – Aggregierte Ansicht



2 Aktivieren Sie eines oder mehrere Kontrollkästchen, um die Kriterien für das Aggregieren der Client-Regeln zu bestimmen, und klicken Sie auf **OK**.

So zeigen Sie die Details einer aggregierten Firewall-Regel an:

- Wählen Sie auf der Registerkarte **Aggregierte Ansicht** eine aggregierte Regel, und klicken Sie auf **Individuelle Regeln anzeigen**.

  Auf der Registerkarte **Standard-Ansicht** werden alle in der aggregierten Regel enthaltenen individuellen Regeln angezeigt.

Konfigurieren der Richtlinie für Quarantäneoptionen

Mithilfe der Richtlinie für die Quarantäneoptionen können Sie den Quarantänemodus aktivieren bzw. deaktivieren, eine Quarantänebenachrichtigung erstellen, isolierte Netzwerke definieren und Fehleroptionen konfigurieren.

So konfigurieren Sie die Richtlinie für Quarantäneoptionen:

1 Wählen Sie in der Konsolenstruktur die Gruppe oder die Computer aus, auf die die Richtlinie angewendet werden soll.

2 Erweitern Sie die Firewall-Funktion, und klicken Sie in der Zeile **Quarantäneoptionen** auf **Bearbeiten**.

Die Liste der Richtliniennamen wird aktiviert.

3 Wählen Sie **Neue Richtlinie**.

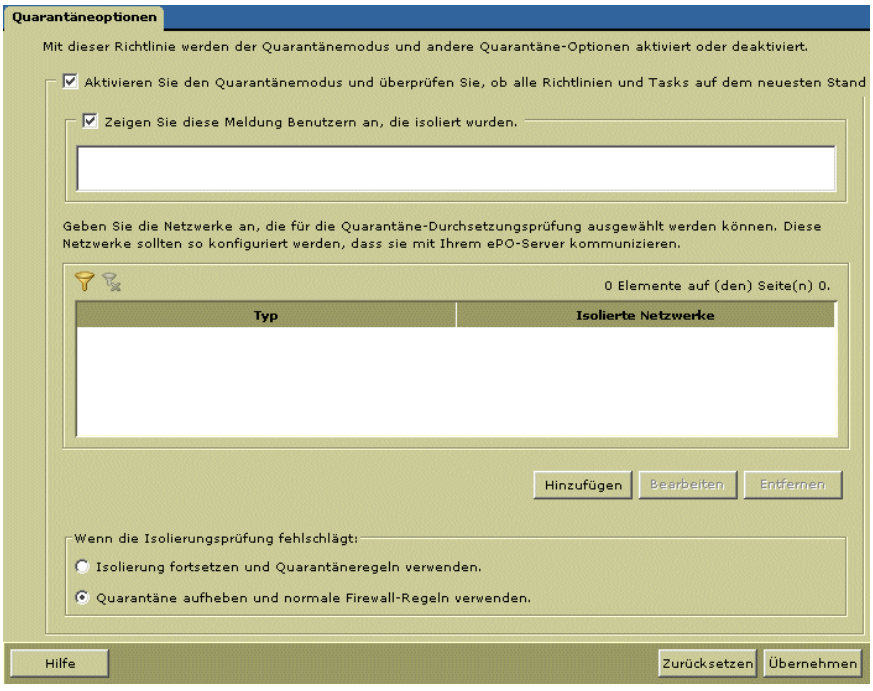
Das Dialogfeld **Neue Richtlinie erstellen** wird geöffnet.

Sie können eine neue duplizierte Richtlinie erstellen, wenn Sie die Einzelheiten zu einer vordefinierten Richtlinie anzeigen, indem Sie unten im Dialogfeld für die Richtlinie auf **Duplizieren** klicken. Geben Sie den Namen der neuen Richtlinie ein, und geben Sie an, ob die Richtlinie augenblicklich dem aktuellen Knoten zugewiesen werden soll.

4 Wählen Sie die Richtlinie, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein, und klicken Sie auf **OK**.

Das Dialogfeld **Quarantäneoptionen** wird geöffnet.

Abbildung 5-13 Quarantäneoptionen


Quarantäneoptionen
Mit dieser Richtlinie werden der Quarantänemodus und andere Quarantäne-Optionen aktiviert oder deaktiviert.
Aktivieren Sie den Quarantänemodus und überprüfen Sie, ob alle Richtlinien und Tasks auf dem neuesten Stand
Zeigen Sie diese Meldung Benutzern an, die isoliert wurden.
Geben Sie die Netzwerke an, die für die Quarantäne-Durchsetzungsprüfung ausgewählt werden können. Diese Netzwerke sollten so konfiguriert werden, dass sie mit Ihrem ePO-Server kommunizieren.
0 Elemente auf (den) Seite(n) 0.
Typ
Isolierte Netzwerke
Hinzufügen
Bearbeiten
Entfernen
Wenn die Isolierungsprüfung fehlschlägt:
Isolierung fortsetzen und Quarantäneregeln verwenden.
Quarantäne aufheben und normale Firewall-Regeln verwenden.
Hilfe
Zurücksetzen
Übernehmen

5 Wählen Sie die entsprechenden Einstellungen.

6 Klicken Sie auf **Anwenden**, und schließen Sie das Dialogfeld.

Der Name der neuen Richtlinie wird in der Richtlinienliste angezeigt.

7 Klicken Sie auf **Übernehmen**.

Konfigurieren der Richtlinie „Quarantäneregeln“

Die Richtlinie „Quarantäneregeln“ stellt einen besonderen Satz von Firewall-Regeln dar, die durchgesetzt werden, wenn der **Quarantänemodus** aktiviert ist. Quarantäneregeln können Sie erstellen und verwalten, indem Sie eine Richtlinie „Quarantäneregeln“ mit den entsprechenden Einstellungen anwenden.

Wenn sich Benutzer mittels VPN-Software mit dem Netzwerk verbinden, sollten Sie sicherstellen, dass die Quarantäneregeln den Datenverkehr zulassen, der für die Verbindung und die Authentifizierung über VPN erforderlich ist.

Sie können die normale Firewall-Funktion verwenden, um festzustellen, welche mit VPN zusammenhängenden Regeln Sie für den **Quarantänemodus** benötigen. Aktivieren Sie den Lernmodus oder den adaptiven Modus, und stellen Sie dann eine VPN-Verbindung her. Die Host Intrusion Prevention generiert automatisch die benötigten VPN-Regeln, die Sie dann in Ihren Quarantäneregeln reproduzieren können.

Die Richtlinie für **Quarantäneregeln** bietet Zugriff auf:

- *Erstellen neuer Richtlinien für Quarantäneregeln*
- *Anzeigen und Bearbeiten von Quarantäneregeln*
- *Erstellen einer neuen Quarantäneregel oder -gruppe*
- *Löschen einer Quarantäneregel oder -gruppe*

Erstellen neuer Richtlinien für Quarantäneregeln

Um eine neue, nicht knotenspezifische Richtlinie hinzuzufügen, müssen Sie die Richtlinie im **Richtlinienkatalog** erstellen. Nähere Informationen dazu finden Sie unter *Richtlinienkatalog* auf Seite 128. Um eine neue, knotenspezifische Richtlinie hinzuzufügen, müssen Sie die in diesem Abschnitt beschriebenen Schritte durchführen.

So erstellen Sie eine Quarantäneregelrichtlinie:

1 Wählen Sie in der Konsolenstruktur die Gruppe oder den Computer aus, auf den die Richtlinie angewendet werden soll.

2 Erweitern Sie die Firewall-Funktion, und klicken Sie in der Zeile **Quarantäneregeln** auf **Bearbeiten**.

Die Liste der Richtliniennamen wird aktiviert.

3 Führen Sie einen der folgenden Vorgänge aus:

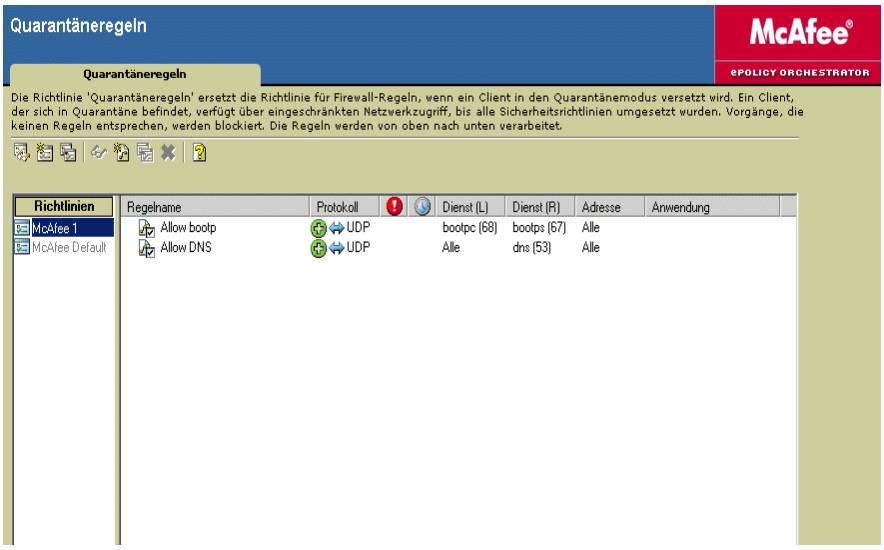
- Wählen Sie in der Liste eine der vorkonfigurierten Richtlinien aus, und klicken Sie auf **Anwenden**.
- Wählen Sie **Neue Richtlinie**, um eine neue Richtlinie zu erstellen.

Das Dialogfeld **Neue Richtlinie erstellen** wird geöffnet.

4 Wählen Sie die Richtlinie aus, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein, und klicken Sie auf **OK**.

Das Dialogfeld **Quarantäneregeln** wird geöffnet. Die neue Richtlinie ist in der Richtlinienliste ausgewählt.

Abbildung 5-14 Dialogfeld „Quarantäneregeln“



5 Führen Sie einen der folgenden Schritte aus:

- Regeln hinzufügen (siehe *Erstellen einer neuen Quarantäneregel oder -gruppe* auf Seite 99).
- Regeln bearbeiten (siehe *Anzeigen und Bearbeiten von Quarantäneregeln* auf Seite 99).
- Regeln entfernen (siehe *Löschen einer Quarantäneregel oder -gruppe* auf Seite 100).

6 Klicken Sie auf **Schließen**, um das Dialogfeld zu schließen.

Der Name der neuen Richtlinie wird in der Richtlinienliste angezeigt.

7 Klicken Sie auf **Anwenden**.

Eine neue Richtlinie können Sie auch im Dialogfeld **Quarantäneregeln** erstellen, indem Sie auf **Richtlinie hinzufügen** oder auf **Richtlinie duplizieren** klicken.

Anzeigen und Bearbeiten von Quarantäneregeln

Sie können die Details einer Regel anzeigen und die Optionen einer Regel bearbeiten. Dies geschieht im Dialogfeld **Quarantäneregeln**.

So zeigen Sie eine Quarantäneregel an und bearbeiten sie:

1 Wählen Sie in der Liste **Richtlinien** eine Richtlinie und dann im Detailbereich die Regel aus, die Sie anzeigen bzw. bearbeiten möchten.

2 Klicken Sie auf **Eigenschaften**.

Das Dialogfeld **Quarantäneregel** wird geöffnet.

3 Ändern Sie die Regeleinstellungen nach Ihren Vorstellungen.

4 Klicken Sie auf **OK**, um die Änderungen zu speichern.

Erstellen einer neuen Quarantäneregel oder -gruppe

Sie können eine völlig neue Regel erstellen oder eine vorhandene Regel duplizieren und bearbeiten. Außerdem können Sie eine Gruppe für eine bestimmte Regelmenge erstellen sowie vordefinierte Regeln hinzufügen. Neue Regeln und Gruppen können Sie im Dialogfeld **Quarantäneregeln** erstellen.

So erstellen Sie eine Quarantäneregel:

1 Klicken Sie auf der Registerkarte **Quarantäneregeln** in der Richtlinie für Quarantäneregeln auf **Hinzufügen** und anschließend auf **Neue Regel**.

Das Dialogfeld **Quarantäne-Firewall-Regel** wird geöffnet.

2 Wählen Sie die entsprechenden Einstellungen.

3 Klicken Sie auf **OK**.

Sie können auch Regeln erstellen, indem Sie zur Richtlinie vordefinierte Regeln und Regelgruppen hinzufügen. Klicken Sie auf **Hinzufügen** und dann auf **Vordefinierte Regeln**. Wählen Sie im Dialogfeld **Vordefinierte Regeln auswählen** die Gruppe oder einzelne Regeln, die Sie hinzufügen möchten. Klicken Sie dann auf **OK**.

So erstellen Sie eine neue Regelgruppe:

1 Klicken Sie auf der Registerkarte **Quarantäneregeln** in der Richtlinie für Quarantäneregeln auf **Hinzufügen** und anschließend auf **Neue Gruppe**.

Das Dialogfeld **Quarantäne-Firewall-Regelgruppe** wird geöffnet.

2 Geben Sie im Feld **Name** einen Namen für die Gruppe ein.

3 Klicken Sie auf **OK**, um die Gruppe hinzuzufügen.

Jetzt können Sie in dieser Gruppe neue Regeln erstellen oder vorhandene Regeln aus der Quarantäne-Firewall-Regelliste in die Gruppe verschieben.

So fügen Sie vordefinierte Regeln hinzu:

1 Klicken Sie auf der Registerkarte **Quarantäneregeln** in der Richtlinie für Quarantäneregeln auf **Hinzufügen** und anschließend auf **Vordefinierte Regeln**.

   Das Dialogfeld **Vordefinierte Regeln auswählen** wird geöffnet.

2 Wählen Sie eine oder mehrere Gruppen oder in einer Gruppe vorhandene Regeln aus.

3 Klicken Sie auf **OK**, um die ausgewählten Gruppen und Regeln hinzuzufügen.

Löschen einer Quarantäneregel oder -gruppe

Regeln und Gruppen können Sie im Dialogfeld **Quarantäneregeln** löschen.

So löschen Sie eine Quarantäneregel oder -gruppe:

1 Wählen Sie die Registerkarte **Quarantäneregeln** in der Richtlinie für Quarantäneregeln, und wählen Sie die zu löschenden Regeln bzw. Gruppen aus.

2 Klicken Sie auf **Löschen**.

3 Klicken Sie im Bestätigungsdialogfeld auf **Ja**, um die Elemente aus der Liste zu entfernen.

6 Anwendungsblockierrichtlinien

Die Anwendungsblockierfunktion in Host Intrusion Prevention verwaltet einen Satz an Anwendungen, die es Ihnen erlauben, andere Anwendungen auszuführen (bezeichnet als Anwendungserstellung) oder eine Bindung zu diesen herzustellen (bezeichnet als Anwendungs-Hooking).

In diesem Abschnitt wird die Anwendungsblockierfunktion beschrieben. Folgende Themen werden behandelt:

- *Übersicht*
- *Konfigurieren der Richtlinie für die Anwendungsblockieroptionen*
- *Konfigurieren der Richtlinie „Anwendungsblockierregeln“*

Übersicht

Die Anwendungsblockierfunktion aktiviert oder deaktiviert die Anwendungsblockierung und konfiguriert Anwendungsblockierregeln. Mit der Anwendungsblockierung können Sie die Anwendungserstellungsblockierung, die Blockierung des Anwendungs-Hooking oder beides festlegen. Sie können auch angeben, ob die Anwendung weiterhin Anwendungsblockierregeln verwenden soll, die auf Clients manuell oder über den adaptiven oder den Lernmodus erstellt wurden.

Anwendungserstellung

Blockieren Sie die Anwendungserstellung, wenn Sie verhindern wollen, dass bestimmte oder unbekannte Programme ausgeführt werden. So können beispielsweise einige Trojaner auf Ihrem Computer ohne Wissen des Benutzers schädliche Programme ausführen. Wenn Sie die Anwendungserstellung blockieren, können Sie diese Art von Angriffen verhindern, indem Sie lediglich zulassen, dass bestimmte, legitimierte Anwendungen ausgeführt werden. Sie können auch den automatischen adaptiven Modus oder den interaktiven Lernmodus aktivieren, um dynamisch einen Satz zugelassener Anwendungen zu erstellen.

Anwendungs-Hooks

Blockieren Sie das Anwendungs-Hooking, um zu verhindern, dass sich unbekannte Anwendungen an andere Programme binden. Dieser Hook-Typ tritt auf Kernelebene der API auf und wird von einigen legitimierten Anwendungen benötigt – er kann aber auch auf einen Angriff hinweisen. So kann z. B. eine schädliche Anwendung versuchen, sich per E-Mail zu versenden, indem Sie einen Hook zur E-Mail-Anwendung herstellt. Sie können diese Angriffe verhindern, indem Sie das Anwendungs-Hooking blockieren oder es so konfigurieren, dass nur bestimmte Anwendungen sich selbst an andere Programme binden. Sie können auch den automatischen adaptiven Modus oder den interaktiven Lernmodus aktivieren, um unbekannte Anwendungen zu behandeln, die einen Hook-Versuch zu anderen Anwendungen unternehmen.

Vordefinierte Anwendungsblockierungsrichtlinien

Die Anwendungsblockierfunktion enthält zwei Richtlinienkategorien:

- **Anwendungsblockieroptionen:** Aktiviert oder deaktiviert die Blockierung der Anwendungserstellung und des -Hooking. Die vordefinierten Richtlinien umfassen **Aus (McAfee-Standard)**, **Ein**, **Adaptiv, Lernmodus**.
- **Anwendungsblockierregeln:** Definiert die Anwendungsblockiereinstellungen. Die vordefinierte Richtlinie ist der Standard **(McAfee-Standard)**.

Direktzugriff

Die Anwendungsblockierfunktion bietet Links (*) für den direkten Zugriff auf die Überwachung und Verwaltung der Anwendungsblockierregeln und der Anwendungsblockierungs-Client-Regeln.

Abbildung 6-1 Anwendungsblockierfunktion

Konfigurieren der Richtlinie für die Anwendungsblockieroptionen

Die Richtlinie für die Anwendungsblockieroptionen besitzt vier vorkonfigurierte Richtlinien, die Sie auswählen können. Alternativ können Sie eine neue Richtlinie erstellen und anwenden.

So wenden Sie eine Richtlinie für die Anwendungsblockieroptionen an:

1 Wählen Sie in der Konsolenstruktur die Gruppe oder die Computer aus, auf die die Richtlinie angewendet werden soll.

2 Erweitern Sie die Funktion **Anwendungsblockierung** und klicken Sie in der Zeile **Anwendungsblockieroptionen** auf **Bearbeiten**.

Die Liste der Richtliniennamen wird aktiviert.

3 Führen Sie einen der folgenden Vorgänge aus:

- Wählen Sie in der Liste eine der vorkonfigurierten Richtlinien aus und klicken Sie auf **Anwenden**:

Wählen Sie folgende Richtlinie...	Für folgende Einstellungen...
Aus (McAfee-Standard)	Alle Einstellungen sind deaktiviert.
Ein	■ Anwendungserstellungsblockierung, Standardschutz ■ Anwendungs-Hook-Blockierung, Standardschutz
Adaptiv	■ Anwendungserstellungsblockierung, Adaptiver Modus ■ Anwendungs-Hook-Blockierung, Adaptiver Modus
Lernen	■ Anwendungserstellungsblockierung, Lernmodus ■ Anwendungs-Hook-Blockierung, Lernmodus

- Wählen Sie **Neue Richtlinie**.

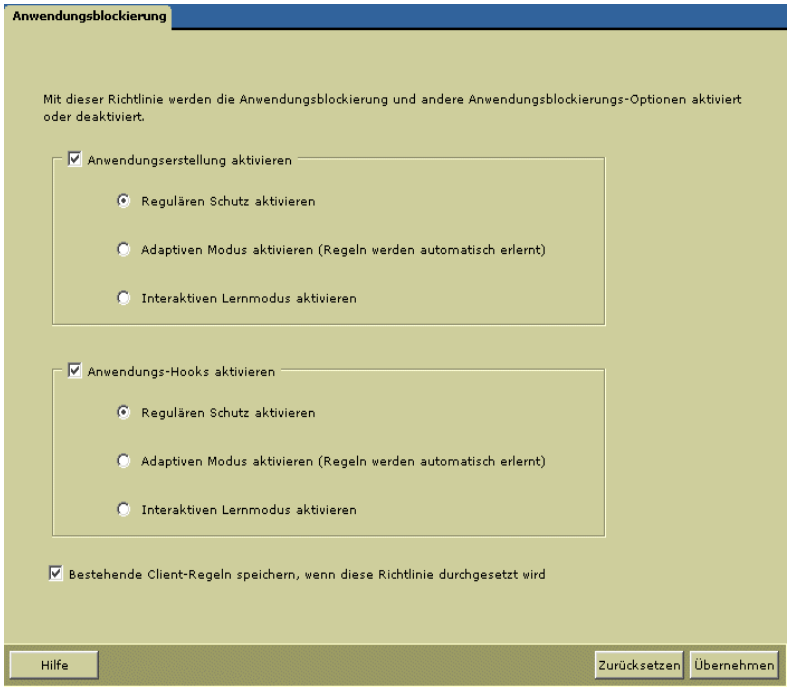
Das Dialogfeld **Neue Richtlinie erstellen** wird geöffnet.

Sie können eine neue duplizierte Richtlinie erstellen, wenn Sie die Einzelheiten zu einer vordefinierten Richtlinie anzeigen, indem Sie unten im Dialogfeld für die Richtlinie auf **Duplizieren** klicken. Geben Sie den Namen der neuen Richtlinie ein und geben Sie an, ob die Richtlinie augenblicklich dem aktuellen Knoten zugewiesen werden soll.

4 Wählen Sie die Richtlinie aus, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein und klicken Sie auf **OK**.

Das Dialogfeld **Anwendungsblockieroptionen** wird geöffnet.

Abbildung 6-2 Anwendungsblockieroptionen



5 Wählen Sie die entsprechenden Einstellungen.

6 Klicken Sie auf **Anwenden** und schließen Sie das Dialogfeld.

Der Name der neuen Richtlinie wird in der Richtlinienliste angezeigt.

7 Klicken Sie auf **Übernehmen**.

Konfigurieren der Richtlinie „Anwendungsblockierregeln“

Regeln legen fest, wie die Anwendungsblockierfunktion die verschiedenen Anwendungen behandelt. Sie können Regeln erstellen und verwalten, indem Sie eine Richtlinie **Anwendungsblockierregeln** mit den entsprechenden Einstellungen anwenden.

Die Richtlinie für **Anwendungsblockierregeln** bietet Zugriff auf:

- *Erstellen neuer Richtlinien für Anwendungsblockierregeln*
- *Anzeigen und Bearbeiten von Anwendungsblockierregeln*
- *Erstellen neuer Anwendungsblockierregeln*
- *Löschen einer Anwendungsblockierregel*
- *Anzeigen von Client-Anwendungsregeln*

Erstellen neuer Richtlinien für Anwendungsblockierregeln

Um eine neue, nicht knotenspezifische Richtlinie hinzuzufügen, müssen Sie die Richtlinie im Richtlinienkatalog erstellen. Nähere Informationen dazu finden Sie unter *Registerkarte „Richtlinien“* auf Seite 126. Um eine neue knotenspezifische Richtlinie hinzuzufügen, müssen Sie die in diesem Abschnitt beschriebenen Schritte durchführen.

So erstellen Sie eine Richtlinie für Anwendungsblockierregeln:

1 Wählen Sie in der Konsolenstruktur die Gruppe oder die Computer aus, auf die Richtlinie angewendet werden soll.

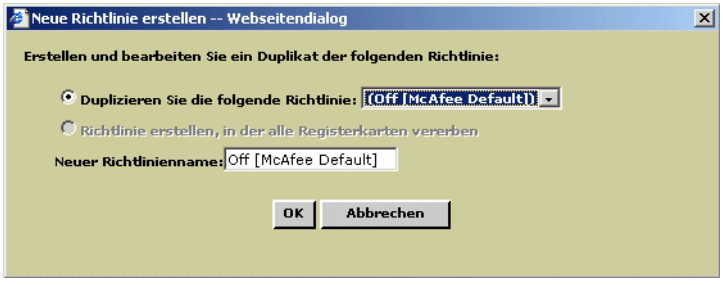
2 Erweitern Sie die Funktion **Anwendungsblockierung** und klicken Sie in der Zeile **Anwendungsblockierregeln** auf **Bearbeiten**.

Die Liste der Richtliniennamen wird aktiviert.

3 Wählen Sie **Neue Richtlinie**.

Das Dialogfeld **Neue Richtlinie erstellen** wird geöffnet.

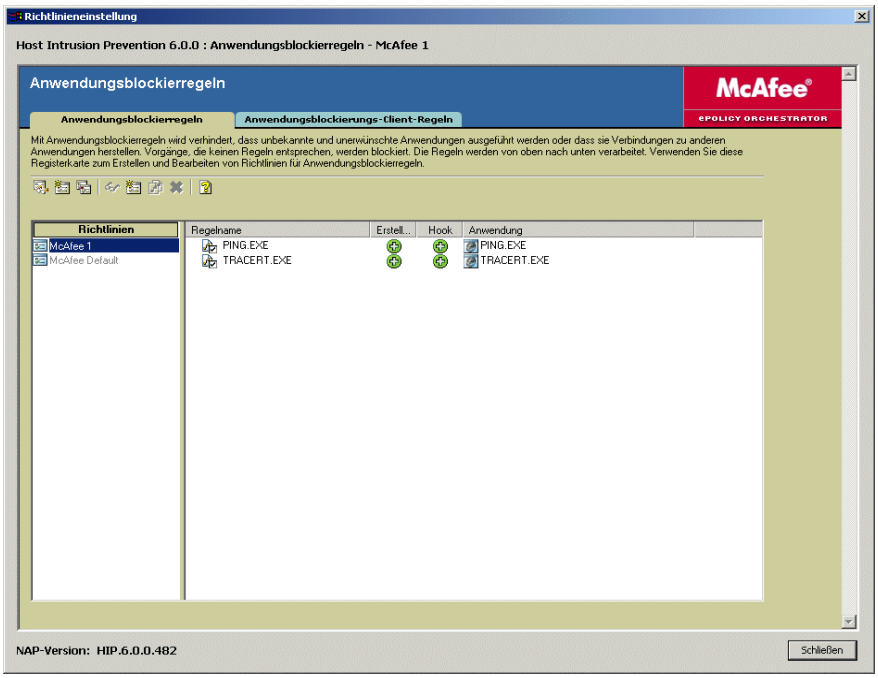
Abbildung 6-3 Dialogfeld „Neue Richtlinie erstellen“


Neue Richtlinie erstellen -- Webseitendialog
Erstellen und bearbeiten Sie ein Duplikat der folgenden Richtlinie:
Duplizieren Sie die folgende Richtlinie:
[Off [McAfee Default]]
Richtlinie erstellen, in der alle Registerkarten vererben
Neuer Richtlinienname:
Off [McAfee Default]
OK
Abbrechen

4 Wählen Sie die Richtlinie aus, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein und klicken Sie auf **OK**.

Das Dialogfeld **Anwendungsblockierregeln** wird geöffnet. Die neue Richtlinie ist in der Richtlinienliste ausgewählt.

Abbildung 6-4 Dialogfeld „Anwendungsblockierregeln“



5 Führen Sie einen der folgenden Schritte aus:

- Regeln hinzufügen (siehe *Erstellen neuer Anwendungsblockierregeln* auf Seite 107).
- Regeln bearbeiten (siehe *Anzeigen und Bearbeiten von Anwendungsblockierregeln*).
- Regeln entfernen (siehe *Löschen einer Anwendungsblockierregel* auf Seite 108).

6 Klicken Sie auf **Schließen**, um das Dialogfeld zu schließen.

Der Name der neuen Richtlinie wird in der Richtlinienliste angezeigt.

7 Klicken Sie auf **Anwenden**.

Eine neue Richtlinie können Sie auch im Dialogfeld **Anwendungsblockierregeln** erstellen, indem Sie auf **Richtlinie hinzufügen** oder auf **Richtlinie duplizieren** klicken.

Anzeigen und Bearbeiten von Anwendungsblockierregeln

Sie können die Details einer Regel anzeigen oder eine Regel bearbeiten, um sie zu deaktivieren, anzupassen und die Anwendungsoptionen zu ändern. Sie können die Regeln auf der Registerkarte **Anwendungsblockierregeln** in der Richtlinie „Anwendungsblockierregeln“ anzeigen und bearbeiten.

So zeigen Sie eine Anwendungsblockierregel an und bearbeiten sie:

1 Wählen Sie auf der Registerkarte **Anwendungsblockierregeln** eine Richtlinie aus der Liste **Richtlinien** aus und wählen Sie anschließend im Detailbereich die Regel aus, die Sie anzeigen oder bearbeiten möchten.

2 Klicken Sie auf **Eigenschaften**.

Das Dialogfeld **Anwendungsregel** wird geöffnet.

3 Ändern Sie die Regeleinstellungen nach Ihren Vorstellungen. Einzelheiten zu den einzelnen Einstellungen finden Sie unter *Erstellen neuer Anwendungsblockierregeln*:

4 Klicken Sie auf **OK**, um die Änderungen zu speichern.

Erstellen neuer Anwendungsblockierregeln

Sie können eine völlig neue Regel erstellen oder eine vorhandene Regel duplizieren und bearbeiten. Neue Regeln können Sie im Dialogfeld **Anwendungsblockierregeln** auf der Registerkarte **Anwendungsregeln** erstellen.

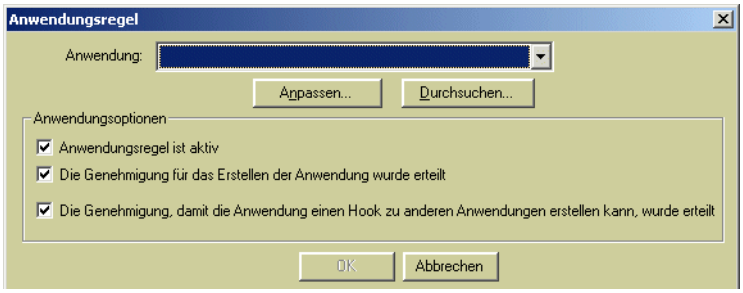
So erstellen Sie eine neue Anwendungsblockierregel:

1 Klicken Sie auf der Registerkarte **Anwendungsblockierregeln** in der Richtlinie „Anwendungsblockierregeln“ auf **Hinzufügen**.

Sie können auch eine neue Regel erstellen, indem Sie eine vorhandene Regel auswählen, auf **Duplizieren** klicken, die Regel bearbeiten und speichern.

Das Dialogfeld **Anwendungsregel** wird geöffnet.

Abbildung 6-5 Dialogfeld „Anwendungsregel“



2 Wählen Sie die Anwendung, auf die diese Regel angewendet werden soll, in der **Anwendungsliste** aus. Wenn die Anwendung nicht in der Liste angezeigt wird, klicken Sie auf **Durchsuchen**, um zu der Programmdatei der Anwendung zu navigieren.

3 Klicken Sie auf **Anpassen**, um zu konfigurieren, wie die Anwendung mit der Regel übereinstimmen muss, und wählen Sie anschließend eine der folgenden Optionen aus:

- **Fingerabdruck der Anwendung:** Berechnet eine Prüfsumme der Anwendung auf dem Server, mit dem nur dann eine Übereinstimmung vorliegt, wenn die Client-Anwendung exakt die Version der zugehörigen Anwendung auf dem Server besitzt.
- **Der Pfad bei erster Übereinstimmung, aber dann der Fingerabdruck:** Wenn die Anwendung zum ersten Mal gestartet wird, wird die Übereinstimmung auf der Grundlage des vom Benutzer angegebenen Pfads ermittelt. Wenn dieser übereinstimmt, wird für den Client der Fingerabdruck berechnet. Ab diesem Punkt wird die Übereinstimmung mit der Regel nur noch auf der Grundlage des Fingerabdrucks der Anwendung ermittelt.

- **Immer der Pfad und nicht der Fingerabdruck:** Wenn die Anwendung gestartet wird, wird die Übereinstimmung auf der Grundlage des vom Benutzer angegebenen Pfads ermittelt.

- Durch Klicken auf **Durchsuchen** können Sie zu den Anwendungen auf dem ePO-Server navigieren. In den meisten Fällen müssen Sie auf **Anpassen** klicken und die entsprechenden Optionen auswählen, um sicherzustellen, dass die richtige Anwendung auf dem Client-System angewendet wird.

4 Wählen Sie die **Anwendungsoptionen**:

Wählen Sie die Option...	Aktion
Anwendungsregel ist aktiv	Aktiviert diese Regel.
Die Genehmigung für das Erstellen der Anwendung wurde erteilt	Die Anwendung darf ausgeführt werden.
Die Genehmigung, damit die Anwendung einen Hook zu anderen Anwendungen erstellen kann, wurde erteilt	Die Anwendung darf sich mit anderen Anwendungen verbinden.

5 Klicken Sie auf **OK**, um die neue Regel zur Liste **Anwendungsregeln** hinzuzufügen.

Löschen einer Anwendungsblockierregel

Regeln können Sie in der Richtlinie „Anwendungsblockierregeln“ auf der Registerkarte **Anwendungsblockierregeln** löschen.

So löschen Sie eine Anwendungsblockierregel:

1 Wählen Sie auf der Registerkarte **Anwendungsblockierregeln** in der Richtlinie „Anwendungsblockierregeln“ eine oder mehrere zu löschende Regeln aus.

2 Klicken Sie auf **Löschen**.

3 Klicken Sie im Bestätigungsdialogfeld auf **Ja**, um die Regeln aus der Liste zu entfernen.

Wenn Sie eine Regel löschen, wird diese permanent entfernt. Wir empfehlen, die Regel zu bearbeiten und die Auswahl von **Aktiv** aufzuheben, um die Regel zu deaktivieren.

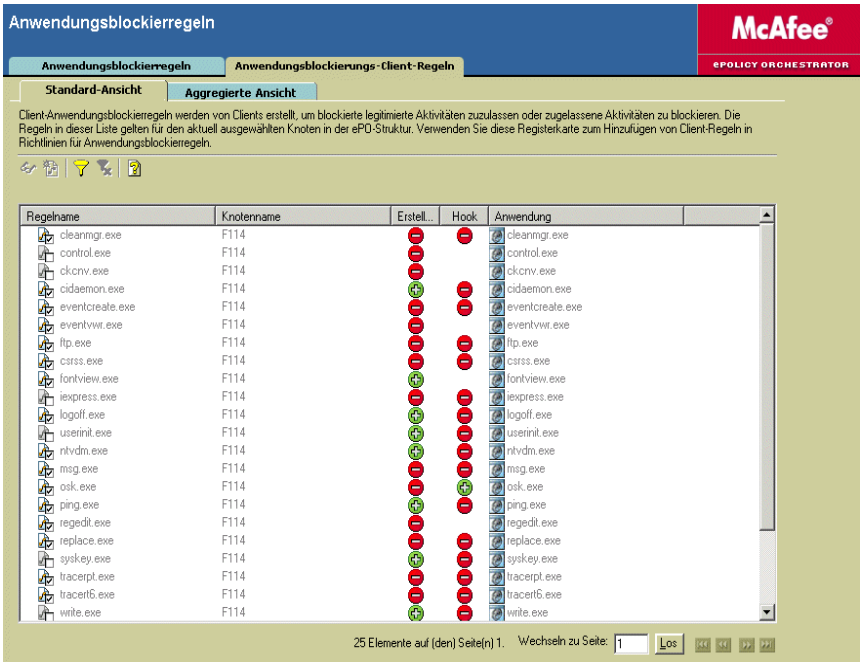
Anzeigen von Client-Anwendungsregeln

Auf der Registerkarte **Anwendungsblockierungs-Client-Regeln** werden alle auf Client-Systemen erstellten Regeln angezeigt, mit denen Anwendungen erlaubt oder blockiert werden. In der **Standard-Ansicht** werden alle Regeln, einschließlich der Duplikate, angezeigt. In der **Aggregierten Ansicht** werden Regeln in Gruppen mit ähnlichen Merkmalen angezeigt.

So zeigen Sie alle Client-Anwendungsregeln an:

1 Wählen Sie in der Richtlinie „Anwendungsblockierregeln“ die Registerkarte **Anwendungsblockierungs-Client-Regeln** aus und klicken Sie auf die Registerkarte **Standard-Ansicht**.

Abbildung 6-6 Registerkarte „Standard-Ansicht“


Anwendungsblockierregeln
McAfee
ePOLICY ORCHESTRATOR
Anwendungsblockierregeln
Anwendungsblockierungs-Client-Regeln
Standard-Ansicht
Aggregierte Ansicht
Client-Anwendungsblockierregeln werden von Clients erstellt, um blockierte legitimierte Aktivitäten zuzulassen oder zugelassene Aktivitäten zu blockieren. Die Regeln in dieser Liste gelten für den aktuell ausgewählten Knoten in der ePO-Struktur. Verwenden Sie diese Registerkarte zum Hinzufügen von Client-Regeln in Richtlinien für Anwendungsblockierregeln.
Regelname
Knotenname
Erstell...
Hook
Anwendung
25 Elemente auf (den) Seite(n) 1.
Wechseln zu Seite:
Los

2 Führen Sie einen der folgenden Schritte aus, um die Ansicht zu ändern:

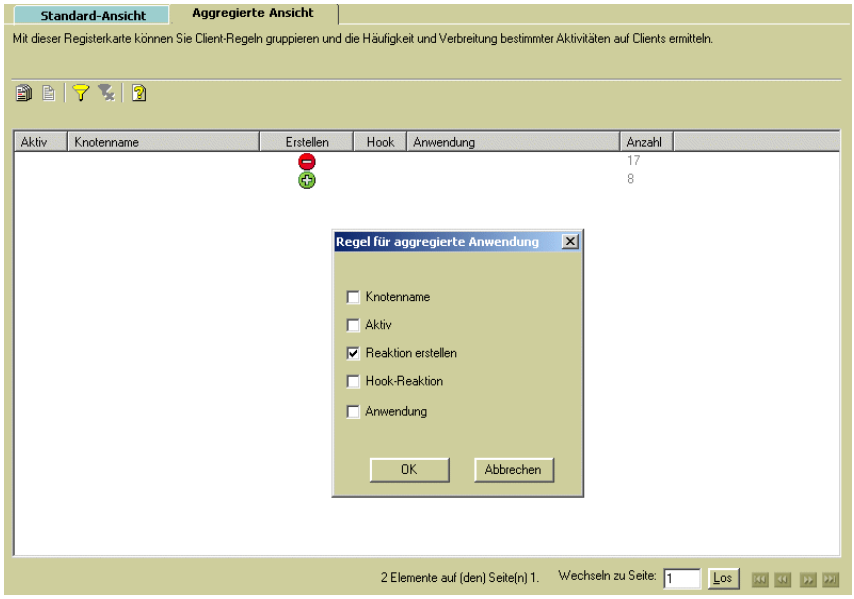
Ziel	Aktion...
Details einer Regel anzeigen	Wählen Sie die Regel aus und klicken Sie auf **Eigenschaften**.
Eine Regel zu einer Richtlinie verschieben	Wählen Sie die Regel aus und klicken Sie auf **Zu Richtlinie hinzufügen**.
Die Liste der Regeln durchblättern	Klicken Sie in der Symbolleiste auf die Navigationsschaltflächen.
Die Liste der Regeln filtern	Klicken Sie auf **Filter festlegen**. Aktivieren Sie im Dialogfeld **Anwendungsfilter festlegen** eines oder mehrere Kontrollkästchen und geben Sie einen Wert in das entsprechende Feld ein, um einen Filter festzulegen.

So zeigen Sie aggregierte Client-Anwendungsregeln an:

1 Wählen Sie in der Richtlinie „Anwendungsblockierregeln“ die Registerkarte **Anwendungsblockierungs-Client-Regeln** aus und klicken Sie auf die Registerkarte **Aggregierte Ansicht**.

2 Klicken Sie auf **Spalte auswählen**, damit das Dialogfeld **Aggregierte Anwendungsregel** geöffnet wird (falls es nicht bereits angezeigt wird).

Abbildung 6-7 Registerkarte „Aggregierte Ansicht“



3 Aktivieren Sie eine oder mehrere Optionen, um die Kriterien für das Aggregieren der Client-Regeln zu bestimmen und klicken Sie auf **OK**.

So zeigen Sie die Details einer aggregierten Client-Anwendungsregel an:

- Wählen Sie auf der Registerkarte **Aggregierte Ansicht** eine aggregierte Regel und klicken Sie im Kontextmenü oder in der Symbolleiste auf **Individuelle Regeln anzeigen**.

  Auf der Registerkarte **Standard-Ansicht** werden alle in der aggregierten Regel enthaltenen individuellen Regeln angezeigt.

7 Allgemeine Richtlinien

Die Funktion „Allgemein“ der Host Intrusion Prevention bietet Zugriff auf Richtlinien allgemeiner Art, die sich nicht nur auf einzelne Funktionen beziehen.

In diesem Abschnitt wird die Funktion „Allgemein“ beschrieben. Folgende Themen werden behandelt:

- *Übersicht*
- *Konfigurieren von „Richtlinien erzwingen“*
- *Konfigurieren der Richtlinie „Client-UI“*
- *Konfigurieren der Richtlinie „Vertrauenswürdige Netzwerke“*
- *Konfigurieren der Richtlinie „Vertrauenswürdige Anwendungen“*

Übersicht

Allgemeine Richtlinien gelten für IPS- und Firewall-Einstellungen und haben Priorität über Einstellungen in einzelnen IPS- und Firewall-Richtlinien.

Die Richtlinie **Richtlinien erzwingen** bildet die grundlegende Funktion zum Ein- bzw. Ausschalten der administrativen Host Intrusion Prevention-Richtlinien auf dem Client.

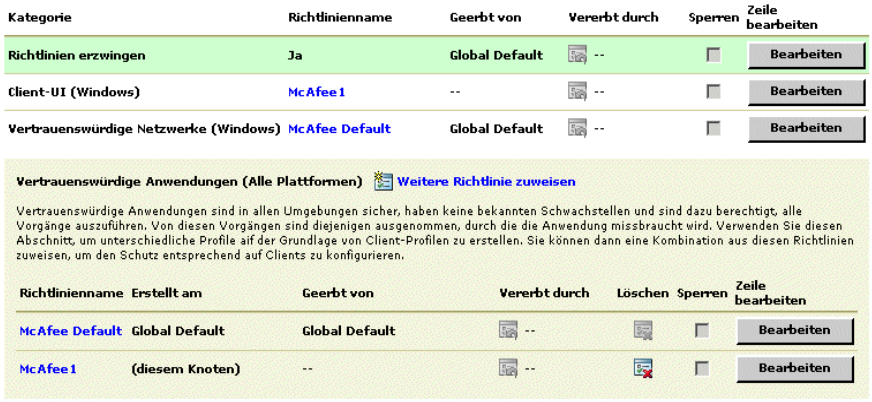
Die Richtlinie **Client-UI** bestimmt, welche Optionen auf einem Client-Computer mit Host IntrusionPrevention-Client verfügbar sind. Sie legt auch fest, ob das Client-Symbol in der Taskleiste angezeigt wird, welche Typen von Intrusionswarnungen angezeigt werden und mit welchen Kennwörtern der Zugriff auf die Client-Oberfläche möglich ist.

Die Richtlinie **Vertrauenswürdige Netzwerke** listet die IP-Adressen und Subnetze auf, mit denen die Kommunikation als sicher eingestuft ist. Zu den vertrauenswürdigen Netzwerken können Subnetze, einzelne IP-Adressen oder IP-Adressbereiche gehören. Durch das Markieren von Netzwerken als „vertrauenswürdig“ sind weniger oder keine IPS-Ausnahmen und zusätzliche Firewall-Regeln mehr erforderlich.

Die Richtlinie **Regeln für vertrauenswürdige Anwendungen** listet die Anwendungen auf, die sicher sind, bei denen keine bekannten Schwachstellen vorliegen und die berechtigt sind, alle Vorgänge auszuführen. Durch das Markieren von Anwendungen als „vertrauenswürdig“ sind weniger oder keine IPS-Ausnahmen und zusätzliche Firewall- und Anwendungsblockierregeln mehr erforderlich. Diese Richtlinienkategorie kann ebenso wie die Richtlinie **IPS-Regeln** (siehe *Konfigurieren der Richtlinie für IPS-Regeln* auf Seite 44) mehrere Richtlinieninstanzen enthalten.

Die Einstellungen für die Richtlinie **Vertrauenswürdige Netzwerke** und für die Richtlinie **Vertrauenswürdige Anwendungen** reduziert die Anzahl von Falsch-Positiv-Meldungen und unterstützt damit das Tunen einer Bereitstellung.

Abbildung 7-1 Funktion „Allgemein“



Vordefinierte Richtlinien „Allgemein“

Die Funktion „Allgemein“ enthält vier Richtlinienkategorien:

- **Erzwingen von Richtlinien:** Aktiviert oder deaktiviert die administrative Richtliniendurchsetzung. Die vordefinierten Richtlinien umfassen **Ja (McAfee-Standard)** und **Nein**.
- **Client-UI:** Definiert den Zugriff auf die Client-Benutzeroberfläche der Host Intrusion Prevention. Die vordefinierte Richtlinie ist die Standardrichtlinie **(McAfee-Standard)**.
- **Vertrauenswürdige Netzwerke:** Erstellt vertrauenswürdige Netzwerke. Die vordefinierte Richtlinie ist die Standardrichtlinie **(McAfee-Standard)**.
- **Vertrauenswürdige Anwendungen:** Definiert vertrauenswürdige Anwendungen. Die vordefinierte Richtlinie ist die Standardrichtlinie **(McAfee-Standard)**.

Konfigurieren von „Richtlinien erzwingen“

Diese Richtlinie bildet die grundlegende Funktion zum Ein- bzw. Ausschalten des Erzwingens von Richtlinien. Diese Richtlinie kann weder gelöscht noch bearbeitet werden. Es können auch keine neuen Richtlinien erstellt werden.

So ändern Sie die Richtlinienkonfiguration:

1 Wählen Sie in der Konsolenstruktur die Gruppe oder die Computer aus, auf die die Richtlinie angewendet werden soll.

2 Erweitern Sie die Funktion **Allgemein**, und klicken Sie in der Zeile **Richtlinien erzwingen** auf **Bearbeiten**.

Die Liste der Richtliniennamen wird aktiviert.

3 Wählen Sie **Nein** oder **Ja**.

Der Standard **Ja** ermöglicht es, administrative Richtlinien auf Clients durchzusetzen; **Nein** verhindert das Erzwingen administrativer Richtlinien.

Wenn die Richtlinie auf **Nein** eingestellt ist, deaktiviert dies den Client und die Schutzfunktion für dessen Hosts nicht. Diese Einstellung verhindert lediglich, dass auf dem Client Richtlinienaktualisierungen erzwungen werden.

Abbildung 7-2 Erzwingen von Richtlinien

4 Klicken Sie auf **Übernehmen**.

Konfigurieren der Richtlinie „Client-UI“

Die Client-UI-Richtlinie bestimmt, welche Optionen auf einem Windows-Client-Computer verfügbar sind, der durch Host Intrusion Prevention geschützt ist. Dazu gehören die Einstellungen für die Symbolanzeige, die Reaktionen auf Intrusionsereignisse und der Administrator- und Client-Benutzer-Zugriff.
Mit den Optionen dieser Richtlinie können die Anforderungen von drei typischen Benutzerrollen erfüllt werden:

Normaler Benutzer

Dies ist der durchschnittliche Benutzer, auf dessen PC oder Laptop der Host Intrusion Prevention-Client installiert ist. Die Richtlinie „Client-UI“ versetzt den Benutzer in die Lage, folgende Aktionen durchzuführen:

- Anzeigen des Host Intrusion Prevention-Client-Symbols in der Taskleiste und Starten der Client-Benutzeroberfläche.
- Erhalten von Popup-Intrusionswarnungen oder Deaktivieren der Popups nach deren Einblendung.
- Erstellen zusätzlicher IPS-, Firewall- und Anwendungsblockierregeln.

Getrennter Benutzer

Dies ist ein Benutzer, der eventuell mit einem Laptop arbeitet und dessen Verbindung mit dem Host Intrusion Prevention-Server für eine bestimmte Zeit getrennt ist. Dieser Benutzer kann technische Probleme mit der Host Intrusion Prevention haben, oder er muss Vorgänge ohne Interaktion mit der Host Intrusion Prevention durchführen. Mithilfe der Richtlinie „Client-UI“ kann dieser Benutzer ein computerspezifisches zeitbasiertes Kennwort erhalten, mit dem er Verwaltungs-Tasks durchführen oder Schutzfunktionen ein- oder ausschalten kann.

Administratorbenutzer

Dies ist ein IT-Administrator für alle Computer, der auf einem Client-Computer besondere Vorgänge durchführen muss, bei denen alle administratorberechtigten Richtlinien überschrieben werden. Mithilfe der Richtlinie „Client-UI“ kann dieser Benutzer ein unbefristetes Administratorkennwort erhalten, mit dem er Verwaltungs-Tasks durchführen kann.

Zu den Verwaltungs-Tasks für getrennte Benutzer und Administratorbenutzer gehören:

- Aktivieren bzw. Deaktivieren von IPS-, Firewall- und Anwendungsblockierrichtlinien.
- Erstellen zusätzlicher IPS-, Firewall- und Anwendungsblockierregeln in Fällen, wo bestimmte legitimierte Aktivitäten blockiert werden.

Über die ePolicy Orchestrator-Konsole vorgenommene Änderungen der Verwaltungsrichtlinie werden erst durchgesetzt, wenn das Kennwort abgelaufen ist. Während dieser Zeit erstellte Client-Regeln werden gespeichert, sofern dies durch Verwaltungsregeln zugelassen wird.

Erstellen und Anwenden einer Client-UI-Richtlinie

Wenn die standardmäßige Client-UI-Richtlinie nicht nach Ihren Vorstellungen konfiguriert ist, können Sie eine neue Richtlinie erstellen und die entsprechenden Optionen auswählen. Sie können die Richtlinie dann auf einen oder eine Gruppe von Computern anwenden.

So konfigurieren Sie eine Client-UI-Richtlinie:

1. Wählen Sie in der Konsolenstruktur die Gruppe oder die Computer aus, auf die neue Richtlinie angewendet werden soll.
2. Erweitern Sie die Funktion **Allgemein**, und klicken Sie in der Zeile **Client-UI** auf **Bearbeiten**.

   Die Liste der Richtliniennamen wird aktiviert.
3. Wählen Sie **Neue Richtlinie**.

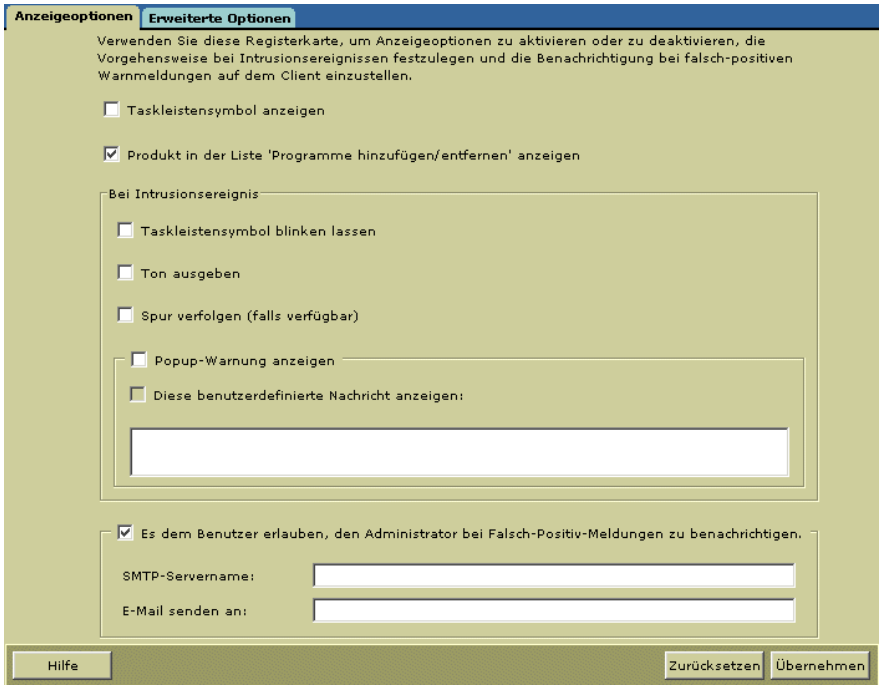
   Das Dialogfeld **Neue Richtlinie erstellen** wird geöffnet.

Erstellen Sie eine neue duplizierte Richtlinie, wenn Sie die Einzelheiten zu einer vordefinierten Richtlinie anzeigen, indem Sie unten im Dialogfeld für die Richtlinie auf **Duplizieren** klicken. Geben Sie den Namen der neuen Richtlinie ein, und geben Sie an, ob die Richtlinie augenblicklich dem aktuellen Knoten zugewiesen werden soll.

4 Wählen Sie die Richtlinie, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein, und klicken Sie auf **OK**.

Das Dialogfeld **Client-UI** wird geöffnet.

Abbildung 7-3 Client-UI – Registerkarte „Anzeigeoptionen“


Anzeigeoptionen
Erweiterte Optionen
Verwenden Sie diese Registerkarte, um Anzeigeoptionen zu aktivieren oder zu deaktivieren, die Vorgehensweise bei Intrusionsereignissen festzulegen und die Benachrichtigung bei falsch-positiven Warnmeldungen auf dem Client einzustellen.
Taskleistensymbol anzeigen
Produkt in der Liste 'Programme hinzufügen/entfernen' anzeigen
Bei Intrusionsereignis
Taskleistensymbol blinken lassen
Ton ausgeben
Spur verfolgen (falls verfügbar)
Popup-Warnung anzeigen
Diese benutzerdefinierte Nachricht anzeigen:
Es dem Benutzer erlauben, den Administrator bei Falsch-Positiv-Meldungen zu benachrichtigen.
SMTP-Servername:
E-Mail senden an:
Hilfe
Zurücksetzen
Übernehmen

5 Ändern Sie die Einstellungen nach Ihren Vorstellungen. Klicken Sie auf **Hilfe**, wenn Sie allgemeine Details nachlesen wollen. Details zu Kennwörtern erhalten Sie unter *Kennwörter einrichten* auf Seite 115; Details zur Taskleistensteuerung finden Sie unter *Taskleistensteuerung* auf Seite 117.

6 Klicken Sie auf **OK**, um die Änderungen zu speichern.

Einzelheiten über die Arbeit mit der Client-Oberfläche finden Sie unter *Host Intrusion Prevention-Client* auf Seite 142.

Kennwörter einrichten

In der Client-UI-Richtlinie legen Sie das Kennwort fest, mit dem die Client-UI auf einem Client-Computer entsperrt werden kann. Das Kennwort wird aktiviert, sobald die Richtlinie auf den Client angewendet wird.

Es sind zwei Kennworttypen verfügbar:

- Ein Administratorkennwort, das von einem Administrator konfiguriert werden kann und das so lange gültig ist, wie die Richtlinie auf den Client angewendet wird. Die Client-UI ist weiterhin entsperrt, bis sie geschlossen wird. Um die Client-UI wieder zu öffnen, geben Sie das Administratorkennwort erneut ein. Um ein Administratorkennwort zu erstellen und anzuwenden, wählen Sie eine Website, Gruppe oder einen Computer in der Verzeichnisstruktur aus.

- Ein zeitbasiertes Kennwort, das automatisch generiert wird, das nur für einen bestimmten Computer gilt und zu einem vorgegebenen Zeitpunkt abläuft. Die Client-UI ist weiterhin entsperrt, auch wenn sie geschlossen ist, solange das zeitbasierte Kennwort gültig ist. Um ein zeitbasiertes Kennwort zu erstellen und anzuwenden, wählen Sie einen einzelnen Computer in der Verzeichnisstruktur aus.

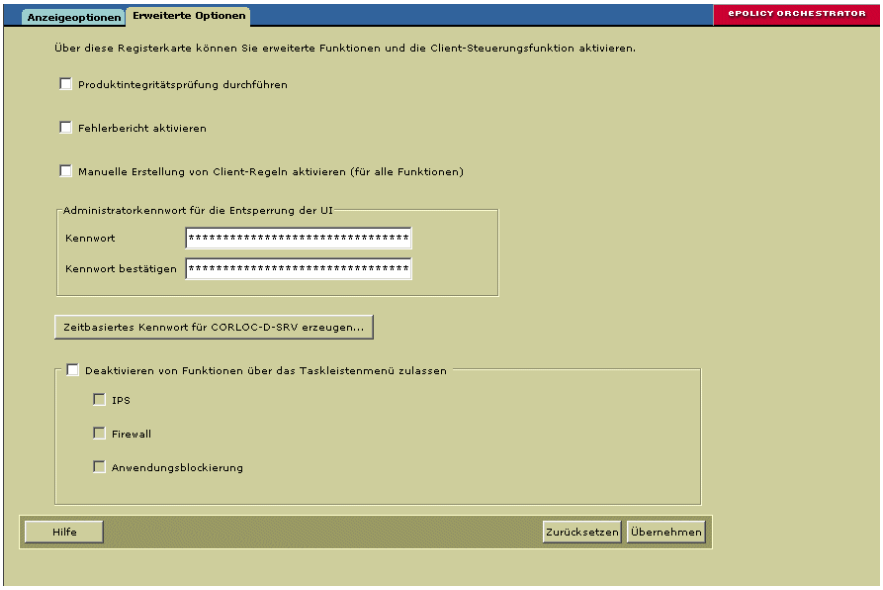
Richtlinien werden nur auf dem Client erzwungen, wenn der Client geschlossen ist, unabhängig davon, ob der Client gesperrt oder entsperrt ist.

Einzelheiten zur Verwendung eines Kennwortes für die Entsperrung der Client-UI finden Sie unter *Entsperren der Client-Benutzeroberfläche* auf Seite 144.

So erstellen Sie ein Administratorkennwort:

1 Klicken Sie in der Richtlinie „Client-UI“ auf die Registerkarte **Erweiterte Optionen**.

Abbildung 7-4 Client-UI – Registerkarte „Erweiterte Optionen“



2 Geben Sie das Kennwort in das Textfeld **Kennwort** ein. Es muss mindestens zehn Zeichen lang sein.

3 Geben Sie das Kennwort noch einmal in das Textfeld **Kennwort bestätigen** ein.

4 Klicken Sie auf **Übernehmen**.

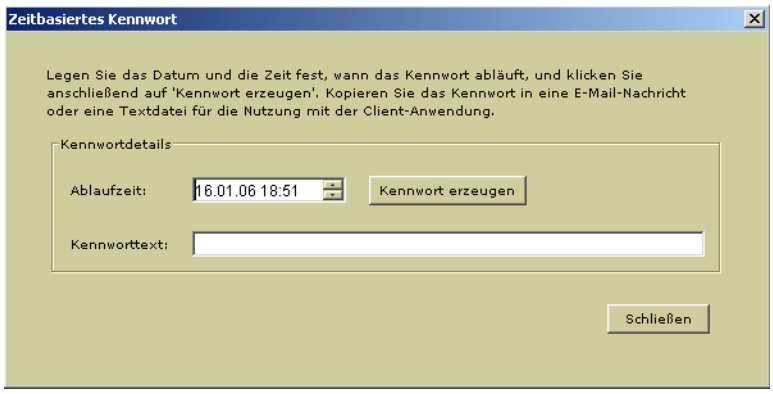
Wenn Sie das Administratorkennwort auf dem Client verwenden, müssen Sie immer das Kontrollkästchen **Administratorkennwort** aktivieren.

So erstellen Sie ein zeitbasiertes Kennwort:

1 Klicken Sie im Dialogfeld der Client-UI-Richtlinie auf die Registerkarte **Erweiterte Optionen** und dann auf **Zeitbasiertes Kennwort erzeugen**.

Das Dialogfeld **Zeitbasiertes Kennwort** wird geöffnet.

Abbildung 7-5 Dialogfeld „Zeitbasiertes Kennwort“


Zeitbasiertes Kennwort
Legen Sie das Datum und die Zeit fest, wann das Kennwort abläuft, und klicken Sie anschließend auf 'Kennwort erzeugen'. Kopieren Sie das Kennwort in eine E-Mail-Nachricht oder eine Textdatei für die Nutzung mit der Client-Anwendung.
Kennwortdetails
Ablaufzeit:
16.01.06 18:51
Kennwort erzeugen
Kennworttext:
Schließen

2 Geben Sie das Datum und die Uhrzeit des Zeitpunktes ein, an dem das Kennwort abläuft, und klicken Sie auf **Kennwort erzeugen**.

Im Textfeld **Kennwort** wird ein kodiertes Kennwort angezeigt.

Taskleistensteuerung

Wenn Benutzer gelegentlich eine Host Intrusion Prevention-Funktion deaktivieren müssen, um auf eine legitime, aber blockierte Anwendung oder Netzwerk-Website zuzugreifen, können sie beispielsweise das Host Intrusion Prevention-Taskleistensymbol verwenden, um eine Funktion zu deaktivieren, ohne die Client-UI zu öffnen, wofür ein Kennwort erforderlich ist.

Details zur Verwendung des Taskleistensymbolmenüs finden Sie unter *Symbol in Systemablage* auf Seite 143.

So ermöglichen Sie die Taskleistensteuerung der Windows-UI:

1 Wählen Sie **Taskleistensymbol anzeigen** auf der Registerkarte **Anzeigeoptionen**.

2 Wählen Sie **Deaktivieren von Funktionen über das Taskleistenmenü zulassen** auf der Registerkarte **Erweiterte Optionen**, und wählen Sie anschließend eine oder alle Funktionen aus, um sie zu deaktivieren.

Nachdem die Richtlinie auf den Client angewendet wird, erscheint das Host Intrusion Prevention-Symbol in der Systemablage, und das Menü wird erweitert, sodass es die Funktion zum Deaktivieren und Wiederherstellen von Optionen beinhaltet. Die deaktivierte Funktion bleibt weiterhin deaktiviert, bis sie durch den Menübefehl wiederhergestellt oder durch eine neue Richtlinie (mit aktivierter Funktion) auf den Client gepushed wird.

Beachten Sie Folgendes:

- Durch Deaktivierung von IPS werden sowohl der Host-IPS- als auch der Netzwerk-IPS-Schutz deaktiviert.
- Durch Deaktivierung der Anwendungsblockierung werden sowohl der Schutz für die Anwendungserstellungsblockierung als auch für die Anwendungs-Hook-Blockierung deaktiviert.
- Wenn die Client-UI geöffnet ist, haben die Menübefehle keine Wirkung.

Konfigurieren der Richtlinie „Vertrauenswürdige Netzwerke“

Mithilfe der Richtlinie Vertrauenswürdige Netzwerke können Sie eine Liste mit Adressen und Subnetzen verwalten, die Sie als vertrauenswürdig einstufen. Mit dieser Richtlinie können Sie:

- Optionen für vertrauenswürdige Netzwerke einrichten.
- Adressen oder Subnetze zur Liste hinzufügen oder daraus löschen.

Wenn ein vertrauenswürdiges Netzwerk eine bestimmte IP-Adresse für Netzwerk-IPS als vertrauenswürdig einstuft und ein anderes vertrauenswürdiges Netzwerk dieselbe IP-Adresse für Netzwerk-IPS als nicht vertrauenswürdig einstuft, hat wie bei den Firewall-Regeln der obere Eintrag Priorität.

So konfigurieren Sie Optionen für vertrauenswürdige Netzwerke:

1 Wählen Sie in der Konsolenstruktur die Gruppe oder die Computer aus, auf die die Richtlinie angewendet werden soll.

2 Erweitern Sie die Funktion **Allgemein**, und klicken Sie in der Zeile **Vertrauenswürdiges Netzwerk** auf **Bearbeiten**.

Die Liste der Richtliniennamen wird aktiviert.

3 Wählen Sie **Neue Richtlinie**.

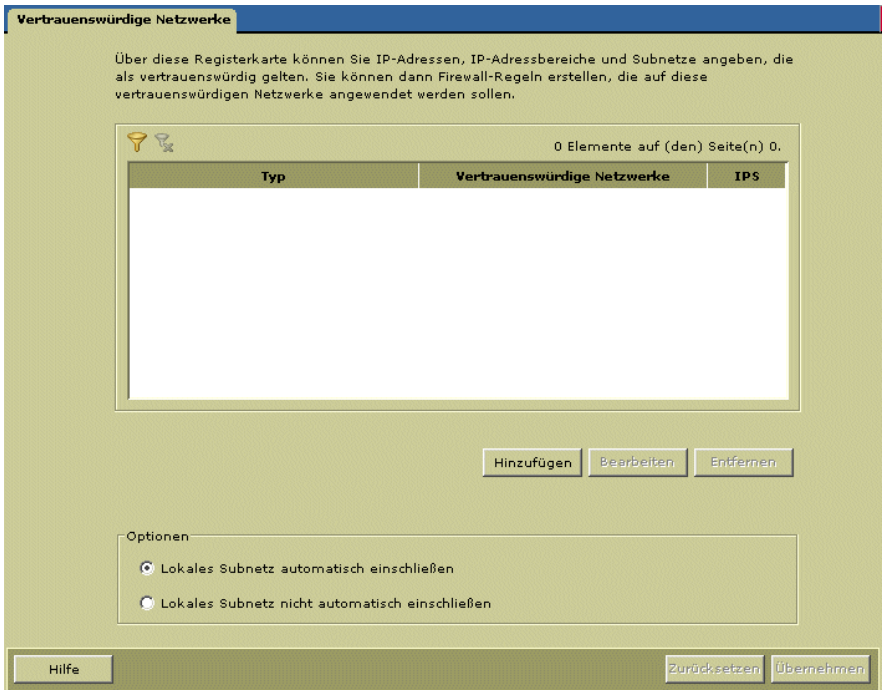
Das Dialogfeld **Neue Richtlinie erstellen** wird geöffnet.

Erstellen Sie eine neue duplizierte Richtlinie, wenn Sie die Einzelheiten zu einer vordefinierten Richtlinie anzeigen, indem Sie unten im Dialogfeld für die Richtlinie auf **Duplizieren** klicken. Geben Sie den Namen der neuen Richtlinie ein, und geben Sie an, ob die Richtlinie augenblicklich dem aktuellen Knoten zugewiesen werden soll.

4 Wählen Sie die Richtlinie aus, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein, und klicken Sie auf **OK**.

Das Dialogfeld **Vertrauenswürdige Netzwerke** wird geöffnet.

Abbildung 7-6 Vertrauenswürdige Netzwerke



5 Führen Sie einen der folgenden Schritte aus:

Wählen Sie...	Aktion
Hinzufügen	Fügen Sie eine vertrauenswürdige Netzwerkadresse zur Liste hinzu. Wählen Sie den Adresstyp aus (Einzel, Bereich, Subnetz), geben Sie die entsprechende Adresse ein, und wählen Sie aus, ob eine Markierung als vertrauenswürdig für Netzwerk-IPS erfolgen soll.
Bearbeiten	Ändern Sie die Daten der ausgewählten vertrauenswürdigen Netzwerkadresse.
Entfernen	Entfernt eine ausgewählte vertrauenswürdige Netzwerkadresse.
Lokales Subnetz automatisch einschließen	Behandelt alle Benutzer desselben Subnetzes automatisch als vertrauenswürdig – auch wenn sie nicht in der Liste enthalten sind.
Lokales Subnetz nicht automatisch einschließen	Behandelt nur in der Liste enthaltene Benutzer als vertrauenswürdig – auch wenn sich diese in demselben vertrauenswürdigen Subnetz befinden.

6 Klicken Sie auf **Anwenden**, und schließen Sie das Dialogfeld.

Der Name der neuen Richtlinie wird in der Richtlinienliste angezeigt.

7 Klicken Sie auf **Übernehmen**.

Konfigurieren der Richtlinie „Vertrauenswürdige Anwendungen“

Über die Richtlinie „Vertrauenswürdige Anwendungen“ können Sie eine Liste der vertrauenswürdigen Anwendungen erstellen. Setzen Sie eine oder mehrere profilbasierte Richtlinien mit diesen Anwendungseinstellungen durch, um die Anzahl an Falsch-Positiv-Meldungen stark zu reduzieren.

Erstellen und Anwenden der Richtlinie „Vertrauenswürdige Anwendungen“

Erstellen und Anwenden der Richtlinie „Vertrauenswürdige Anwendungen“, die vertrauenswürdige Anwendungen definiert. Sie können eine völlig neue Richtlinie oder eine auf einer bestehenden Richtlinie basierende erstellen.

So erstellen Sie eine neue Richtlinie:

1 Erweitern Sie die Funktion **Allgemein**, und klicken Sie in der Zeile **Anwendungsregeln** auf **Bearbeiten**.

Die Liste der Richtliniennamen wird aktiviert.

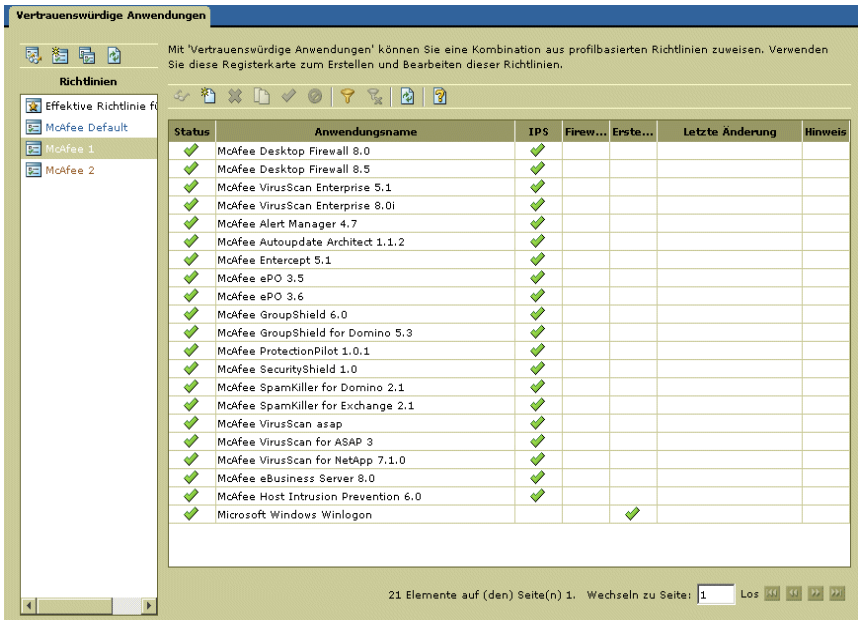
2 Wählen Sie **Neue Richtlinie**.

Das Dialogfeld **Neue Richtlinie erstellen** wird geöffnet.

3 Wählen Sie die Richtlinie, die dupliziert werden soll, geben Sie den Namen der neuen Richtlinie ein, und klicken Sie auf **OK**.

Die Registerkarte **Vertrauenswürdige Anwendung** wird angezeigt.

Abbildung 7-7 Registerkarte „Vertrauenswürdige Anwendung“



4 Ändern Sie die Einstellungen nach Ihren Vorstellungen. Klicken Sie auf **Hilfe**, um Details nachzuschlagen.

5 Klicken Sie auf **Schließen**, um die Änderungen zu speichern.

Erstellen vertrauenswürdiger Anwendungen

Beim Tunen einer Bereitstellung ist das Erstellen von IPS-Ausnahmeregeln ein Weg, um die Anzahl von Falsch-Positiv-Meldungen zu reduzieren. Dies ist nicht immer praktisch, wenn es um mehrere tausend Clients geht oder nur ein begrenzter Zeitraum und Ressourcen zur Verfügung stehen. Die bessere Lösung besteht darin, eine Liste der vertrauenswürdigen Anwendungen zu erstellen, die innerhalb einer bestimmten Umgebung als sichere Anwendungen gelten. Wenn Sie beispielsweise eine Datensicherungsanwendung ausführen, löst dies eine Vielzahl von Falsch-Positiv-Meldungen aus. Um dies zu vermeiden, geben Sie die Datensicherungsanwendung als vertrauenswürdige Anwendung an.

Auch eine vertrauenswürdige Anwendung kann von verbreiteten Schwachstellen, wie einem Pufferüberlauf oder einer illegalen Verwendung, betroffen sein. Aus diesem Grund wird auch eine vertrauenswürdige Anwendung überwacht und kann bestimmte Ereignisse auslösen, um Schwachstellen zu schützen.

So erstellen Sie eine vertrauenswürdige Anwendung:

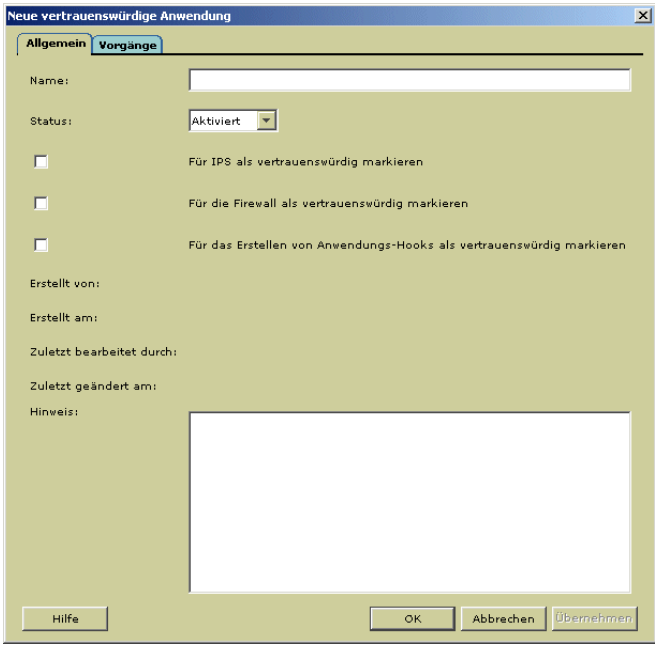
1 Führen Sie auf der Registerkarte **Vertrauenswürdige Anwendung** eine der folgenden Aktionen aus:

- Klicken Sie in der Symbolleiste oder im Kontextmenü auf **Erstellen**. Das Dialogfeld **Neue vertrauenswürdige Anwendung** wird geöffnet.
- Wählen Sie in der Symbolleiste oder im Kontextmenü eine Anwendung aus der Liste aus, und klicken Sie auf **Duplizieren**. Das vorbelegte Dialogfeld **Vertrauenswürdige Anwendung duplizieren** wird geöffnet.

Sie können auch vertrauenswürdige Anwendungen erstellen, die auf einem Ereignis basieren. Einzelheiten hierzu finden Sie unter *Ereignisbasierte Ausnahmen und vertrauenswürdige Anwendungen erstellen* auf Seite 66.

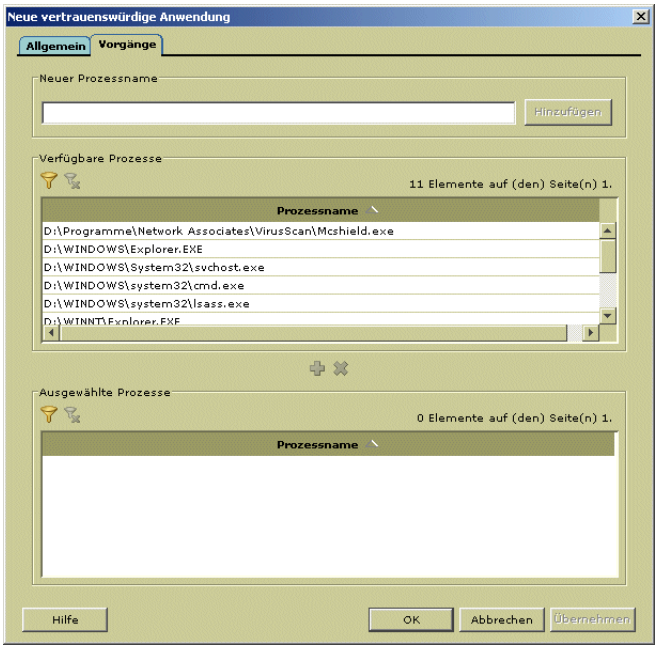
2 Geben Sie auf der Registerkarte **Allgemein** den Namen und den Status ein, und legen Sie fest, ob die Anwendung für die IPS-, Firewall- und das Anwendungs-Hooking vertrauenswürdig ist. Klicken Sie auf **Hilfe**, um Details nachzuschlagen.

Abbildung 7-8 Dialogfeld „Neue vertrauenswürdige Anwendung“ – Registerkarte „Allgemein“



3 Wählen Sie auf der Registerkarte **Vorgänge** diejenigen Vorgänge aus, die vertrauenswürdige Anwendung übernehmen sollen. Klicken Sie auf **Hilfe**, um Details nachzuschlagen.

Abbildung 7-9 Dialogfeld „Neue vertrauenswürdige Anwendung“ – Registerkarte „Allgemein“



4 Klicken Sie auf **OK**.

Vertrauenswürdige Anwendungen bearbeiten

Sie können auch die Eigenschaften einer vorhandenen vertrauenswürdigen Anwendung anzeigen und bearbeiten.

So bearbeiten Sie die Eigenschaften einer vertrauenswürdigen Anwendung:

1 Doppelklicken Sie auf der Registerkarte **Vertrauenswürdige Anwendung** auf eine vertrauenswürdige Anwendung.

Das Dialogfeld **Eigenschaften der vertrauenswürdigen Anwendung** wird geöffnet.

2 Ändern Sie auf den Registerkarten **Allgemein** und **Prozess** die gewünschten Daten, und klicken Sie anschließend auf **OK**.

Vertrauenswürdige Anwendungen aktivieren oder deaktivieren

Anstatt nicht verwendete vertrauenswürdige Anwendungen zu löschen, können Sie diese vorübergehend deaktivieren und später dann erneut aktivieren.

So deaktivieren bzw. aktivieren Sie eine vertrauenswürdige Anwendung:

1 Wählen Sie auf der Registerkarte **Vertrauenswürdige Anwendung** die vertrauenswürdige Anwendung aus, die aktiviert oder deaktiviert werden soll.

2 Klicken Sie in der Symbolleiste oder im Kontextmenü auf **Deaktivieren** bzw. auf **Aktivieren**.

Der Status der Anwendung ändert sich entsprechend auf der Registerkarte **Vertrauenswürdige Anwendung**.

Vertrauenswürdige Anwendungen löschen

Um eine vertrauenswürdige Anwendung permanent zu löschen, wählen Sie diese auf der Registerkarte **Vertrauenswürdige Anwendung** aus, und klicken Sie in der Symbolleiste oder im Kontextmenü auf **Löschen**.

8 Wartung

In diesem Abschnitt werden die für die Wartung und Feineinstellung einer Host Intrusion Prevention-Bereitstellung anfallenden Aktivitäten beschrieben. Folgende Themen werden behandelt:

- *Feineinstellung einer Bereitstellung*
- *Richtlinienverwaltung und Tasks*
- *Ausführen von Server-Tasks*
- *Einrichten von Benachrichtigungen für Ereignisse*
- *Ausführen von Berichten*
- *Aktualisieren von*

Feineinstellung einer Bereitstellung

Nachdem Sie die Clients mit den Standardeinstellungen bereitgestellt haben, können Sie die Feineinstellung vornehmen und die Sicherheit für optimalen Schutz erhöhen. Die Feineinstellung einer Bereitstellung beinhaltet:

- *Analysieren von IPS-Ereignissen*.
- *Erstellen von Ausnahmeregeln und Regeln für vertrauenswürdige Anwendungen*.
- *Mit Client-Ausnahmeregeln arbeiten*.
- *Erstellen und Anwenden neuer Richtlinien*.

Analysieren von IPS-Ereignissen

Ein IPS-Ereignis wird ausgelöst, sobald ein von der Signatur definierter Sicherheitsverstoß erkannt wird. Es wird auf der Registerkarte **IPS-Ereignisse** mit einem Schweregrad von „Hoch“, „Mittel“, „Gering“ oder „Information“ angezeigt, der einer Reaktion zugeordnet ist.

Wenn ein einzelner Vorgang zwei Ereignisse auslöst, wird das Ereignis mit der stärkeren Reaktion ausgewählt.

Bestimmen Sie anhand der Liste der generierten Ereignisse, welche davon kein Risiko darstellen und welche auf verdächtiges Verhalten hinweisen. Um Ereignisse zuzulassen, müssen Sie das System wie folgt konfigurieren:

- **Ausnahmen** – erlauben oder blockieren Sie Regeln, die eine Signaturregel überschreiben.
- **Vertrauenswürdige Anwendungen** – lassen interne Anwendungen zu, deren Vorgänge durch eine Signatur blockiert werden könnten.

Mir dieser Feineinstellung können Sie Falsch-Positiv-Meldungen auf ein Minimum reduzieren und so mehr Zeit für die Analyse ernster Ereignisse verfügbar machen. Weitere Einzelheiten finden Sie unter *IPS-Ereignisse* auf Seite 60.

Erstellen von Ausnahmeregeln und Regeln für vertrauenswürdige Anwendungen

Nach der Analyse der Liste der IPS-Ereignisse können Sie Ausnahmeregeln oder Regeln für vertrauenswürdige Anwendungen für jedes Falsch-Positiv-Ereignis nach Benutzerprofil erstellen. Dies hält die Liste der Ereignisse auf einem minimalen Stand und ermöglicht ein besseres Verständnis schädlicher Angriffe, was sicherstellt, dass die Systeme gegen derartige Angriffe geschützt sind.

Auf der Registerkarte **IPS-Ereignisse** können Sie auf der Grundlage eines bestimmten Ereignisses eine Ausnahme oder eine vertrauenswürdige Anwendung erstellen. Genauere Informationen dazu finden Sie unter *Ereignisbasierte Ausnahmen und vertrauenswürdige Anwendungen erstellen* auf Seite 66.

Mit Client-Ausnahmeregeln arbeiten

Ein einfacher Ansatz für das Erstellen von Ausnahmen ist es, Clients in den adaptiven Modus zu versetzen und es Clients zu erlauben, automatisch Client-Ausnahmeregeln zu erstellen, um harmloses Verhalten zu erlauben. Alle Client-Regeln werden auf der Registerkarte **Client-Regeln** in der Richtlinie **IPS-Regeln** angezeigt. Auch in den Richtlinien **Firewall-Regeln** und **Anwendungsblockierregeln** werden die im adaptiven Modus und im Lernmodus erstellten Client-Regeln angezeigt.

Um die am häufigsten generierten Regeln zu erhalten, verwenden Sie die aggregierte Ansicht der Client-Regeln, in der ähnliche Regeln gruppiert sind. Die Regeln können dann zu den Verwaltungsrichtlinien verschoben werden.

Einzelheiten zur Arbeit mit Client-Regeln finden Sie unter:

- *IPS-Client-Regeln* auf Seite 68.
- *Konfigurieren der Richtlinie für Firewall-Regeln* auf Seite 87.
- *Konfigurieren der Richtlinie „Anwendungsblockierregeln“* auf Seite 105.

Erstellen und Anwenden neuer Richtlinien

Nach dem Erstellen neuer Ausnahmeregeln und vertrauenswürdiger Anwendungen können Sie diese gegebenenfalls zu den vorhandenen Richtlinien hinzufügen. Sie können außerdem neue IPS-Richtlinien und Richtlinien für vertrauenswürdige Anwendungen auf der Grundlage der Richtlinie erstellen, die die Erstellung von Ausnahmen und vertrauenswürdigen Anwendungen erforderlich gemacht hat.

Einzelheiten zum Erstellen und Anwenden neuer Richtlinien finden Sie unter:

- *Konfigurieren der Richtlinie für IPS-Regeln* auf Seite 44.
- *Konfigurieren der Richtlinie für Firewall-Regeln* auf Seite 87.
- *Konfigurieren der Richtlinie „Anwendungsblockierregeln“* auf Seite 105.

Richtlinienverwaltung und Tasks

ePolicy Orchestrator bietet in der Konsolenstruktur zwei Stellen, von denen aus Sie Richtlinien und Tasks von Host Intrusion Prevention anzeigen und verwalten können:

- *Registerkarte „Richtlinien“* eines ausgewählten Knotens in der Konsolenstruktur.
- Die Seite *Richtlinienkatalog*.

Registerkarte „Richtlinien“

Verwenden Sie die Registerkarte **Richtlinien**, um die zu einem ausgewählten Knoten gehörenden Richtlinieninformationen anzuzeigen, zu ändern oder zu erstellen. Einzelheiten finden Sie unter:

- *IPS-Richtlinien* auf Seite 36.
- *Firewall-Richtlinien* auf Seite 72.
- *Anwendungsblockierrichtlinien* auf Seite 101.
- *Allgemeine Richtlinien* auf Seite 111.

Richtlinienübernahme und -zuweisung

Auf der Registerkarte „Richtlinien“ können Sie die Richtlinienübernahme sperren oder entsperren, eine unterbrochene Übernahme anzeigen und zurücksetzen sowie Richtlinienzuweisungen von einem Knoten in einen anderen kopieren.

So sperren Sie die Zuweisung einer benutzerdefinierten Richtlinie:

1. Wählen Sie in der Konsolenstruktur eine Gruppe oder einen Computer aus und klicken Sie auf die Registerkarte **Richtlinien**.
2. Erweitern Sie eine Host Intrusion Prevention-Funktion, sodass sie die Richtlinien anzeigt, die dem Knoten zugewiesen sind.
3. Klicken Sie für eine benutzerdefinierte Richtlinie auf **Bearbeiten**.
4. Wählen Sie **Sperren** aus und klicken Sie auf **Anwenden**.

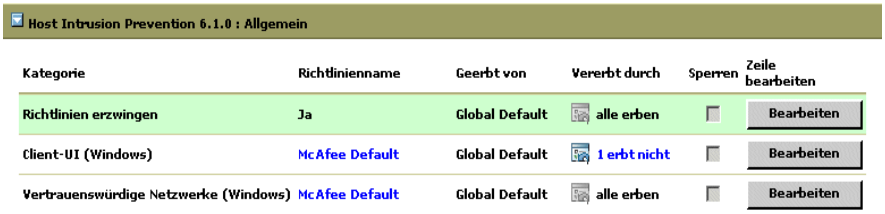
Nur Administratoren können benannte Richtlinien sperren.

So zeigen Sie eine unterhalb eines bestimmten Knotens unterbrochene Übernahme an und setzen diese zurück:

1 Wählen Sie in der Konsolenstruktur eine Gruppe oder einen Computer aus und klicken Sie auf die Registerkarte **Richtlinien**.

2 Erweitern Sie eine Host Intrusion Prevention-Funktion, sodass sie die Richtlinien anzeigt, die dem Knoten zugewiesen sind.

Abbildung 8-1 Richtlinienvererbung



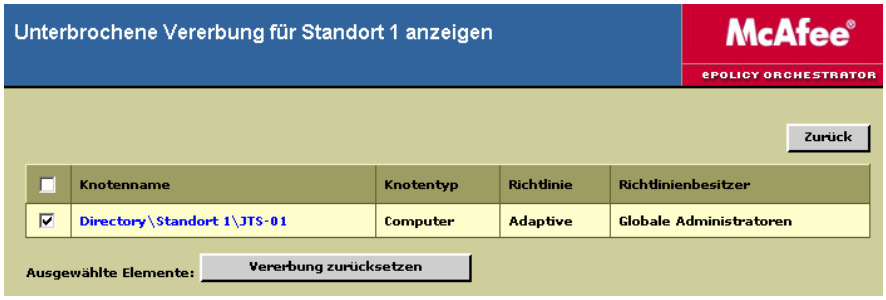
Unter **Übernommen von** wird die Anzahl der Knoten angezeigt, bei denen die Übernahme der Richtlinie unterbrochen ist.

Hierbei handelt es sich um die Anzahl der Knoten, bei denen die Übernahme unterbrochen ist, nicht um die Anzahl der Systeme, die die Richtlinie nicht übernehmen. Beispiel: Wenn nur ein bestimmter Gruppenknoten die Richtlinie nicht übernimmt, wird dies unabhängig von der Anzahl der in der Gruppe vorhandenen Systeme durch **Keine Übernahme: 1** dargestellt.

3 Klicken Sie auf den blauen Text, der die Anzahl der untergeordneten Knoten angibt, die keine Übernahme vornehmen.

Die Seite **Übernahmefehler anzeigen** wird angezeigt, und es werden die Knotennamen aufgeführt.

Abbildung 8-2 Seite „Übernahmefehler anzeigen“



4 Um die Übernahme für einen dieser Knoten erneut zu starten, müssen Sie das Kontrollkästchen neben dem Knotennamen aktivieren und auf **Übernahme zurücksetzen** klicken.

So kopieren Sie die Richtlinienzuweisungen eines Knotens und fügen diese ein:

1 Wählen Sie in der Konsolenstruktur eine Gruppe oder einen Computer aus, von der bzw. dem Sie die Richtlinienzuweisungen kopieren möchten, und klicken Sie auf die Registerkarte **Richtlinien**.

2 Klicken Sie auf **Richtlinienzuweisungen kopieren**.

3 Wählen Sie die Funktionen aus, deren Richtlinienzuweisungen Sie kopieren möchten, und klicken Sie auf **OK**.

4 Wählen Sie in der Konsolenstruktur eine Gruppe oder einen Computer aus und klicken Sie auf **Richtlinienzuweisungen einfügen**.

5 Klicken Sie auf **OK**, um das Ersetzen von Zuweisungen zu bestätigen.

Richtlinienkatalog

Verwenden Sie den Knoten **Richtlinienkatalog** der Konsolenstruktur, um Richtlinien ohne Bezug zu einem bestimmten Knoten anzuzeigen, zu erstellen oder zu bearbeiten.

Anzeigen der Richtlinieninformationen

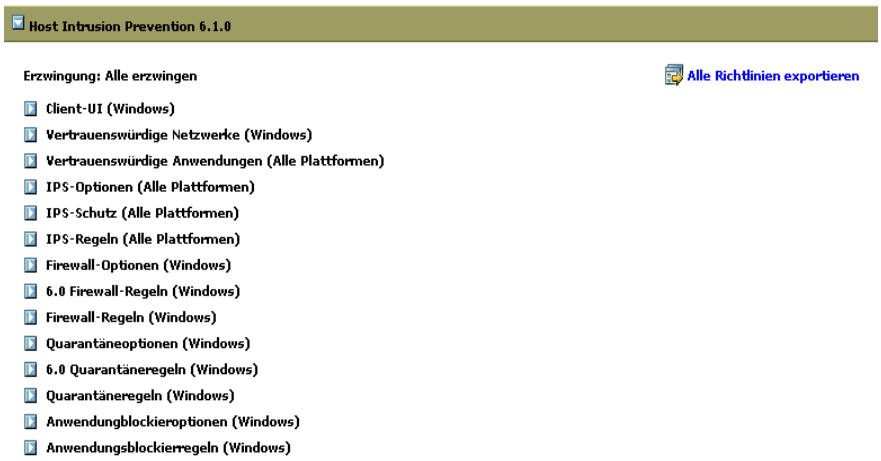
Der Richtlinienkatalog fasst sämtliche Host Intrusion Prevention-Richtlinien zusammen und zeigt deren Zuweisungen und Eigentümer an.

So zeigen Sie alle erstellten Richtlinien an:

1 Wählen Sie in der Konsolenstruktur **Richtlinienkatalog**.

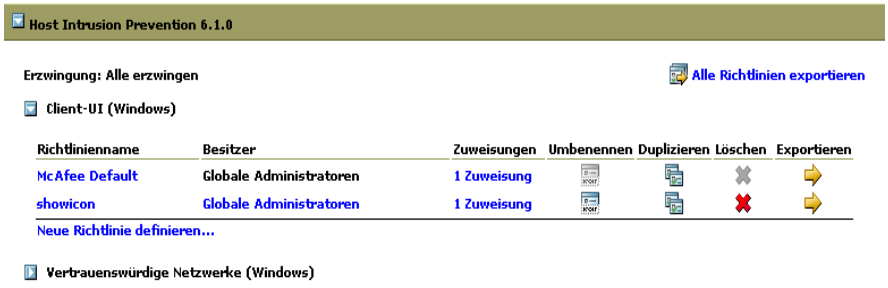
2 Erweitern Sie Host Intrusion Prevention, um die Richtlinienkategorien anzuzeigen.

Abbildung 8-3 Richtlinienkatalog für Host Intrusion Prevention



3 Erweitern Sie eine Richtlinienkategorie, um die Richtlinien für diese Kategorie anzuzeigen.

Abbildung 8-4 Kategorierichtlinien für IPS-Regeln



So zeigen Sie die Knoten an, denen eine Richtlinie zugewiesen ist:

1 Erweitern Sie auf der Seite **Richtlinienkatalog** die Option **Host Intrusion Prevention**, und erweitern Sie anschließend eine Richtlinienkategorie.

2 Klicken Sie in der Zeile der gewünschten benannten Richtlinie unter **Zuweisungen** auf den blauen Text, der die Anzahl der Knoten angibt, denen die Richtlinie zugewiesen ist (beispielsweise **1 Zuweisungen**).

Auf der Seite **Zuweisungen anzeigen** werden alle Knoten, denen die Richtlinie zugewiesen ist, mit ihrem **Knotennamen** und dem **Knotentyp** angezeigt. In dieser Liste sind ausschließlich die Zuweisungspunkte aufgeführt – nicht aber die Knoten, die Richtlinie übernommen haben.

Abbildung 8-5 Zuweisungen für eine Richtlinie anzeigen

3 Klicken Sie auf den Knotennamen, damit die Seite **Richtlinien zuweisen** für den Knoten geöffnet wird.

So zeigen Sie die Einstellungen und den Eigentümer einer Richtlinie an:

1 Erweitern Sie auf der Seite **Richtlinienkatalog** die Option **Host Intrusion Prevention**, und erweitern Sie anschließend eine Richtlinienkategorie.

Unter **Eigentümer** wird der Eigentümer der benannten Richtlinie angezeigt.

2 Klicken Sie auf den Richtliniennamen, um die dazugehörigen Einstellungen anzuzeigen.

So zeigen Sie die Zuweisungen an, bei denen die Richtliniendurchsetzung deaktiviert ist:

1 Klicken Sie auf der Seite **Richtlinienkatalog** auf den blauen Text neben **Durchsetzung**, mit dem die Anzahl der Zuweisungen angegeben wird, deren Durchsetzung deaktiviert ist.

Die Seite **Zuweisungen anzeigen, bei denen die Richtliniendurchsetzung deaktiviert ist** wird geöffnet.

2 Klicken Sie in der Liste auf einen Knoten, damit die Seite **Richtlinien zuweisen** für den Knoten geöffnet wird.

Bearbeiten von Richtlinieninformationen

Auf der Seite **Richtlinienkatalog** können Sie neue benannte Richtlinien erstellen, die standardmäßig keinem bestimmten Knoten zugewiesen sind.

So bearbeiten Sie eine Richtlinie:

1 Erweitern Sie auf der Seite **Richtlinienkatalog** die Option **Host Intrusion Prevention**, und erweitern Sie anschließend eine Richtlinienkategorie.

2 Führen Sie einen der folgenden Schritte aus:

Ziel	Aktion...
Eine Richtlinie erstellen	Klicken Sie auf **Neue Richtlinie definieren**, geben Sie ihr einen Namen, und bearbeiten Sie die Einstellungen.
Eine Richtlinie umbenennen	Klicken Sie auf **Umbenennen**, und bearbeiten Sie den Namen der Richtlinie. (Für die Standardrichtlinie nicht verfügbar.)
Eine Richtlinie duplizieren	Klicken Sie auf **Duplizieren**, bearbeiten Sie den Namen der Richtlinie und deren Einstellungen.
Eine Richtlinie löschen	Klicken Sie auf **Löschen**. (Für die Standardrichtlinie nicht verfügbar.) **Hinweis:** Wenn Sie eine Richtlinie löschen, dann übernehmen alle Knoten, auf die diese Richtlinie aktuell angewendet wird, von ihrem übergeordneten Knoten die Richtlinie derselben Kategorie. Prüfen Sie vor dem Löschen einer Richtlinie sämtliche Knoten, denen diese zugewiesen ist, und weisen Sie diesen eine andere Richtlinie zu, falls Sie nicht wollen, dass nach dem Löschen die Richtlinie des übergeordneten Knotens übernommen wird. Wenn Sie eine Richtlinie löschen, die auf Verzeichnisebene angewendet wird, wird anschließend die Standardrichtlinie der entsprechenden Kategorie angewendet.
Einer Richtlinie einen Eigentümer zuweisen	Klicken Sie auf den Eigentümer der Richtlinie, und wählen Sie in der Liste einen anderen Eigentümer aus. (Für die Standardrichtlinie nicht verfügbar.)
Eine Richtlinie exportieren	Klicken Sie auf **Exportieren**, geben Sie einen Namen ein und speichern Sie die Richtlinie (eine XML-Datei) am gewünschten Speicherort.
Alle Richtlinien exportieren	Klicken Sie auf **Alle Richtlinien exportieren**, geben Sie einen Namen ein und speichern Sie die XML-Richtliniendatei am gewünschten Speicherort.
Richtlinien importieren	Klicken Sie oben auf der Richtlinienkatalogseite auf **Richtlinie importieren**, wählen Sie die XML-Richtliniendatei, und klicken Sie auf **OK**.

Einzelheiten zu den einzelnen Funktionen finden Sie im Produkthandbuch von ePolicy Orchestrator und in der Online-Hilfe.

Ausführen von Server-Tasks

Host Intrusion Prevention bietet die Verwaltung von Server-Tasks und die Beibehaltung der Sicherheitsebene von Clients. Dazu gehören:

- Aktualisieren von Benutzerdomänenlisten (*Verzeichnis-Gateway*)
- Archivieren und Entfernen von Ereignissen aus der Datenbank (*Ereignisarchivierung*)
- Übersetzen von Client-Eigenschaften zur Vereinfachung der Verwaltung (*Eigenschaftenübersetzung*)

Weitere Informationen zum Ausführen von Server-Tasks finden Sie in der Online-Hilfe und im Produkthandbuch von ePolicy Orchestrator.

Verzeichnis-Gateway

Der Verzeichnis-Gateway-Server-Task aktualisiert die Liste der Domänen, auf denen ein Client ausgeführt wird. Die aktualisierte Liste wird beim Erstellen von IPS-Ausnahmeregeln benötigt, weil Regeln nur in den in der Datenbank aufgeführten Domänen durchgesetzt werden. Im Laufe der Zeit werden aber Domänen hinzugefügt oder entfernt. Daher muss die Liste periodisch aktualisiert werden, um sicherzustellen, dass Ausnahmen korrekt angewendet werden.

Wählen Sie für diesen Task in der Liste eine Domäne aus, in der die Aktualisierung ausgeführt werden soll, und geben Sie den erforderlichen Domänenbenutzernamen und das Kennwort ein. Anschließend werden von den entsprechenden Verzeichnisservern Domänen-Updates abgerufen. Dieser Task kann in einem Tages- oder Wochenintervall geplant werden – dies hängt von der Größe Ihrer Umgebung ab. Für eine umfangreichere Bereitstellung sind häufigere Aktualisierungen erforderlich.

Ereignisarchivierung

Durch den Server-Task „Ereignisarchivierung“ werden in der Datenbank enthaltene Ereignisse archiviert und so eine optimale Datenbankleistung erreicht. Mit der Zeit erzeugt Host Intrusion Prevention Tausende von Ereignissen, wodurch die Datenbank stark anwächst. Archivieren Sie ältere Ereignisse, und löschen Sie sie regelmäßig, um die Datenbankgröße zu kontrollieren und das ordnungsgemäße Funktionieren der Anwendung zu gewährleisten.

Geben Sie für diesen Task den Verzeichnispfad für die Speicherung der Archivdatei ein und legen Sie fest, wie viel Tage ein Ereignis mindestens alt sein muss, damit es archiviert wird. Am angegebenen Speicherort wird eine mit dem aktuellen Datum benannte, komprimierte XML-Datei erstellt und die Ereignisse werden aus der Datenbank entfernt.

Eigenschaftenübersetzung

Der Server-Task „Eigenschaftenübersetzung“ übersetzt die Host Intrusion Prevention-Daten, die in der ePolicy Orchestrator-Datenbank gespeichert sind, um das Sortieren, Gruppieren und Filtern von Daten in Host Intrusion Prevention durchzuführen. Dieser Task, der automatisch alle 15 Minuten ausgeführt wird, sollte nicht verändert werden. Sie können diesen Task jedoch, falls erforderlich, deaktivieren.

Um die Häufigkeit zu ändern, mit der der Task ausgeführt wird, deaktivieren Sie den ursprünglichen Task und erstellen Sie einen neuen Server-Task mit einer neuen Häufigkeit.

Einrichten von Benachrichtigungen für Ereignisse

Die Benachrichtigungsfunktion kann Sie bei beliebigen Ereignissen warnen, die auf einem Host Intrusion Prevention-Client oder direkt auf dem Server stattfinden. Sie können Regeln konfigurieren, über die beim Empfangen und Verarbeiten bestimmter Ereignisse auf dem ePolicy Orchestrator-Server E-Mail-, SMS-, Pager- oder SNMP-Trap-Nachrichten gesendet werden. Sie können die Ereigniskategorien angeben, die zur Erstellung einer Benachrichtigung führen, sowie die Häufigkeit, mit der Benachrichtigungen gesendet werden. Sämtliche Einzelheiten hierzu finden Sie in der Online-Hilfe und im Produkthandbuch von ePolicy Orchestrator.

So funktionieren Benachrichtigungen

Wenn innerhalb der Host Intrusion Prevention-Umgebung ein Ereignis eintritt, wird dieses an den ePolicy Orchestrator-Server übergeben. Auf die Ereignisse werden Benachrichtigungsregeln angewendet, die den Gruppen oder der Site zugewiesen sind, die die betroffenen Systeme enthält. Wenn die Bedingungen einer Regel erfüllt sind, wird – abhängig von den in der Regel enthaltenen Vorgaben – eine Benachrichtigungsmeldung gesendet oder ein externer Befehl ausgeführt.

Sie können unabhängige Regeln auf verschiedenen Ebenen im Verzeichnis konfigurieren. Sie können konfigurieren, wann Benachrichtigungen gesendet werden, indem Sie Schwellenwerte festlegen, die auf Aggregationen und Einschränkungen basieren.

ePolicy Orchestrator bietet sechs Standardregeln, die Sie aktivieren und sofort verwenden können. Bevor Sie eine der Standardregeln aktivieren:

1. Geben Sie den E-Mail-Server an, von dem die Benachrichtigungen gesendet werden.
2. Überprüfen Sie, ob die richtige Empfänger-E-Mail-Adresse angegeben ist.

Erstellen von Regeln

Sie können für eine Vielzahl an Ereigniskategorien Regeln erstellen. Dazu gehören:

- Erkannte und blockierte Verletzung einer Zugriffsschutzregel
- Erkannte und NICHT blockierte Verletzung einer Zugriffsschutzregel
- in den Quarantänemodus versetzter Computer
- Gefilterter oder blockierter E-Mail-Inhalt
- Erkannte Intrusion
- Erkannter nicht kompatibler Computer
- Normaler Vorgang
- Fehlgeschlagene Richtliniendurchsetzung
- Fehlgeschlagenes Repository-Update oder fehlgeschlagene Replizierung
- Fehlgeschlagene Softwarebereitstellung
- Erfolgreiche Softwarebereitstellung
- Softwaredefekt oder -fehler
- Unbekannte Kategorie
- Fehlgeschlagenes Update/Upgrade
- Erfolgreiches Update/Upgrade

Alle Regeln werden auf die folgende Art erstellt:

1 Beschreiben der Regel.

2 Festlegen der Filter für die Regel.

3 Festlegen der Schwellen für die Regel.

4 Erstellen der zu sendenden Nachricht und Festlegen der Zustellungsart.

Host Intrusion Prevention-Benachrichtigungen

Host Intrusion Prevention unterstützt die folgenden produktspezifischen Benachrichtigungskategorien:

- Host-Intrusion erkannt und verarbeitet.
- Netzwerkintrusion erkannt und verarbeitet.
- Anwendung blockiert.
- Computer in den Quarantänemodus versetzt.

Benachrichtigungen können nur für alle oder keine der Host- (oder Netzwerk-) IPS-Signaturen erstellt werden. Durch Entercept 5.x unterstützte Benachrichtigungen basieren auf Sätzen von Signatur-IDs oder individuellen Schweregraden. Host Intrusion Prevention unterstützt die Spezifizierung einer einzelnen IPS-Signatur-ID als das Feld **Threat-Name** oder **Regelname** in der Konfiguration der Benachrichtigungsregel. Indem das Signatur-ID-Attribut eines Ereignisses intern einem Threat-Namen zugeordnet wird, wird eine Regel erstellt, anhand derer eine IPS-Signatur eindeutig erkannt werden kann.

Die spezifischen Zuordnungen der Host Intrusion Prevention-Parameter, die im Betreff/Text einer Nachricht erlaubt sind, umfassen Folgendes:

Parameter	Werte für Host- und Netzwerk-IPS-Ereignisse	Werte für blockierte Anwendungsereignisse	Werte für Isolierte Ereignisse
ReceivedThreatNames	SignatureID	Kein	Kein
SourceComputers	Remote-IP-Adresse	Computername	Computername
AffectedObjects	Prozessname	Anwendungsname	IP-Adresse des Computers
EventTimestamp	Zeit des Vorfalls	Zeit des Vorfalls	Zeit des Vorfalls
EventID	ePO-Zuordnung der Ereignis-ID	ePO-Zuordnung der Ereignis-ID	ePO-Zuordnung der Ereignis-ID
AdditionalInformation	Übersetzter Signaturname (eines Client-Computers)	Vollständiger Pfad der Anwendung	Kein

Ausführen von Berichten

Die Host Intrusion Prevention-Software umfasst eine über ePolicy Orchestrator realisierte Berichtsfunktion. Sie können verschiedene nützliche Berichte und Anforderungen für Ereignisse und Eigenschaften erstellen, die vom Client an den Server gesendet und in der Datenbank gespeichert werden.

Die Host Intrusion Prevention-Software enthält vordefinierte Berichts- und Anforderungsvorlagen, die im Berichts-Repository und im Anforderungs-Repository unter **Berichte** in der Konsolenstruktur gespeichert werden. Weitere Informationen finden Sie im *Berichtshandbuch von ePolicy Orchestrator 3.6*.

Um Berichte anzuzeigen, melden Sie sich anhand Ihrer ePO-Anmeldeinformationen bei der Datenbank an. NT-Authentifizierungsdaten werden nicht unterstützt.

Sie können Berichte und Anforderungen für eine Gruppe von ausgewählten Client-Systemen erstellen oder die Berichtsergebnisse nach Produkt- oder Systemkriterien begrenzen. Sie können Berichte in diversen Dateiformaten exportieren, auch in HTML- und Microsoft Excel-Dateien.

Sie können Folgendes tun:

- Einen Verzeichnisfilter festlegen, um nur die ausgewählten Informationen zu sammeln. Auswählen, welches Verzeichnissegment in den Bericht aufgenommen werden soll.
- Einen Datenbankfilter festlegen, in dem Sie mithilfe logischer Operatoren präzise Filterkriterien für die im Bericht zurückgelieferten Daten definieren.
- Grafische Berichte für die in der Datenbank enthaltenen Informationen generieren und diese filtern. Sie können die Berichte drucken und für die Verwendung in anderen Softwareprogrammen exportieren.
- Anforderungen für Computer, Ereignisse und Installationen durchführen.

Vordefinierte Berichte

Die auf den Client-Systemen arbeitenden Host Intrusion Prevention-Clients senden Informationen an den Server, der diese in einer Berichtsdatenbank speichert. Sie führen Berichte und Anforderungen anhand dieser gespeicherten Daten aus.

Es gibt acht vordefinierte Host Intrusion Prevention-Berichte, die in zwei Hauptkategorien unterteilt sind: IPS- und Firewall-Berichte. Sie können über Crystal Reports 8.5 Ihre eigenen Berichtsvorlagen erstellen.

Berichts-Repository

Das Berichts-Repository enthält die in der Host Intrusion Prevention vordefinierten Berichte und Anforderungen sowie die von Ihnen erstellten benutzerdefinierten Berichte und Anforderungen.

Sie können das Berichts-Repository so organisieren und verwalten, dass es Ihren Anforderungen entspricht. Sie können exportierte Berichte als Berichtsvorlagen hinzufügen, um beispielsweise eine beim Generieren eines Berichts vorgenommene benutzerdefinierte Auswahl zu speichern. Oder Sie können benutzerdefinierte Berichtsvorlagen hinzufügen. Sie können Berichtsvorlagen auch in logischen Gruppen organisieren. Sie können z. B. Berichte in Gruppen zusammenfassen, die täglich, wöchentlich oder monatlich ausgeführt werden.

Zusammenfassungsinformationen und Details

Nachdem ein Bericht generiert wurde, wird die in dem von Ihnen gegebenenfalls angegebenen Filter festgelegte Zusammenfassung angezeigt. Ausgehend von der Zusammenfassung können Sie denselben Bericht auf die eine oder zwei Ebenen tiefer liegenden detaillierten Informationen herunterbrechen.

Berichtsinhaltskontrolle

Sie haben die Kontrolle darüber, wie viele Berichtsinformationen für die verschiedenen Benutzer angezeigt werden – beispielsweise für globale Administratoren oder Site-Administratoren. Site-Administratoren oder Site-Prüfer können nur Berichte über Client-Systeme erstellen, die in Sites liegen, für die sie Berechtigungen besitzen. Die Berichtsinformationen werden auch durch das Anwenden von Filtern gesteuert.

Host Intrusion Prevention-Berichte

Zu den Vorlagen für Host Intrusion Prevention-Berichte gehören:

IPS-Berichte	Firewall-Berichte
■ *IPS-Ereigniszusammenfassung nach Signatur* ■ *IPS-Ereigniszusammenfassung nach Ziel* ■ *Netzwerk-Intrusionszusammenfassung nach Quell-IP* ■ *Top 10 der angegriffenen Knoten für IPS* ■ *Top 10 der aufgerufenen Signaturen*	■ *Zusammenfassung der blockierten Anwendungen* ■ *Top 10 der blockierten Anwendungen* ■ *Fehlgeschlagene Quarantäne-Updates*

IPS-Ereigniszusammenfassung nach Signatur

Verwenden Sie diesen Bericht, um IPS-Ereignisse nach Signatur anzuzeigen. Dazu gehören folgende Details:

Ursprüngliche Ansicht	Detailebene 1	Detailebene 2
■ **Signaturname >** ■ Anzahl der Ereignisse	■ Signaturname ■ **Prozess >** ■ Anzahl	■ Betriebssystembenutzer ■ Reaktion ■ Knotenname ■ Quell-IP-Adresse ■ Zeit des Vorfalls ■ Aufzeichnungszeit ■ Schweregrad ■ Ereignisbeschreibung ■ Erweiterte Details

Filter nach Signatur, Aufzeichnungszeit, Schweregrad, Betriebssystembenutzer, Reaktion, Prozess und Ursprungs-IP.

IPS-Ereigniszusammenfassung nach Ziel

Verwenden Sie diesen Bericht, um IPS-Ereignisse pro Host anzuzeigen. Dazu gehören folgende Details:

Ursprüngliche Ansicht	Detailebene 1	Detailebene 2
■ **Host-Name >** ■ Anzahl der Ereignisse	■ Host-Name ■ **Signatur >** ■ Anzahl	■ Betriebssystembenutzer ■ Reaktion ■ Prozess ■ Quell-IP-Adresse ■ Zeit des Vorfalls ■ Aufzeichnungszeit ■ Schweregrad ■ Ereignisbeschreibung ■ Erweiterte Details

Filter nach Signatur, Aufzeichnungszeit, Schweregrad, Betriebssystembenutzer, Reaktion, Prozess und Ursprungs-IP.

Netzwerk-Intrusionszusammenfassung nach Quell-IP

Verwenden Sie diesen Bericht, um Netzwerkintrusionsereignisse nach Ursprungs-IP anzuzeigen. Dazu gehören folgende Details:

Ursprüngliche Ansicht	Detailebene 1	Detailebene 2
■ **Quell-IP-Adresse >** ■ Anzahl der Ereignisse	■ Quell-IP-Adresse ■ **Signaturname >** ■ Anzahl	■ Betriebssystembenutzer ■ Reaktion ■ Prozess ■ Knotenname ■ Quell-IP-Adresse ■ Zeit des Vorfalls ■ Aufzeichnungszeit ■ Schweregrad ■ Ereignisbeschreibung ■ Erweiterte Details

Filter nach Ursprungs-IP, Signatur, Betriebssystembenutzer, Reaktion, Aufzeichnungszeit, Schweregrad und Hostname.

Top 10 der angegriffenen Knoten für IPS

Verwenden Sie diesen Bericht, um ein Balkendiagramm der 10 Hosts anzuzeigen, auf denen die meisten IPS-Ereignisse ausgelöst wurden. Dazu gehören folgende Details:

Ursprüngliche Ansicht	Detailebene 1	Detailebene 2
■ **Host-Name >** ■ Anzahl der Ereignisse	■ Host-Name ■ **Signatur >** ■ Anzahl	■ Betriebssystembenutzer ■ Reaktion ■ Prozess ■ Quell-IP-Adresse ■ Zeit des Vorfalls ■ Aufzeichnungszeit ■ Schweregrad ■ Ereignisbeschreibung ■ Erweiterte Details

Filter nach Plattform und Signaturtyp.

Top 10 der aufgerufenen Signaturen

Verwenden Sie diesen Bericht, um ein Balkendiagramm der 10 am häufigsten ausgelösten IPS-Signaturen anzuzeigen. Dazu gehören folgende Details:

Ursprüngliche Ansicht	Detailebene 1	Detailebene 2
■ **Signaturname >** ■ Anzahl der Ereignisse	■ Signaturname ■ **Prozess >** ■ Anzahl	■ Betriebssystembenutzer ■ Reaktion ■ Knotenname ■ Quell-IP-Adresse ■ Zeit des Vorfalls ■ Aufzeichnungszeit ■ Schweregrad ■ Ereignisbeschreibung ■ Erweiterte Details

Filter nach Plattform und Signaturtyp.

Zusammenfassung der blockierten Anwendungen

Verwenden Sie diesen Bericht, um eine Zusammenfassung der pro Anwendung blockierten Anwendungsereignisse anzuzeigen. Dazu gehören folgende Details:

Ursprüngliche Ansicht	Drilldown
■ **Anwendungsbeschreibung >** ■ Anzahl der Ereignisse	■ Host-Name ■ Host-IP ■ Ereigniszeit ■ Prozessname ■ Anwendungspfad ■ Anwendungsversion ■ Anwendungs-Hash

Filter nach Anwendungsbeschreibung und Ereigniszeit.

Top 10 der blockierten Anwendungen

Verwenden Sie diesen Bericht, um ein Balkendiagramm der 10 am häufigsten blockierten Anwendungen anzuzeigen. Dazu gehören folgende Details:

Ursprüngliche Ansicht	Drilldown
■ **Anwendungsbeschreibung >** ■ Anzahl der Ereignisse	■ Host-Name ■ Host-IP ■ Ereigniszeit ■ Prozessname ■ Anwendungspfad ■ Anwendungsversion ■ Anwendungs-Hash

Filter nach Anwendungsbeschreibung, Hostname und Ereigniszeit.

Fehlgeschlagene Quarantäne-Updates

Verwenden Sie diesen Bericht, um die pro Host fehlgeschlagenen Quarantäne-Updates anzuzeigen. Dazu gehören folgende Details:

Ursprüngliche Ansicht	Drilldown
■ **Host-Name >** ■ Anzahl der Ereignisse	■ Host-Name ■ Host-IP ■ Ereigniszeit

Filter nach Anwendungshostname, Host-IP und Ereigniszeit.

Aktualisieren von

Die ePO-Datenbank enthält Host Intrusion Prevention-Sicherheitsinhaltsdaten, wie z. B. Signaturen, die in den Richtlinien zu Host Intrusion Prevention angezeigt werden. Host Intrusion Prevention unterstützt mehrere Versionen von Client-Inhalten und -Code, wobei der aktuelle verfügbare Inhalt in der ePO-Konsole angezeigt wird. Neue Inhalte werden immer in aufeinander folgenden Versionen unterstützt, sodass Inhaltsupdates hauptsächlich neue Informationen oder geringfügige Änderungen an bestehenden Informationen enthalten.

Updates werden mithilfe eines Inhaltsupdate-Pakets durchgeführt. Dieses Paket enthält Inhaltsversionsinformationen und Skript-Updates. Beim Einchecken wird die Paketversion mit der Version der aktuellen Inhaltsinformationen in der Datenbank verglichen. Wenn das Paket neuer ist, werden die Skripts aus diesem Paket extrahiert und ausgeführt. Diese neuen Inhaltsinformationen werden anschließend bei der nächsten Kommunikation zwischen Agent und Server an Clients weitergeleitet.

Host Intrusion Prevention-Inhaltsupdates müssen für die Verteilung an die Clients in das ePO-Repository eingecheckt werden. Die Host Intrusion Prevention-Clients sollten Updates nur über die Kommunikation mit dem ePO-Server erhalten und nicht direkt über FTP- oder HTTP-Protokolle.

Der grundlegende Prozess umfasst das Einchecken des Inhaltspakets in das ePO-Repository und das Senden der aktualisierten Informationen an die Clients.

Einchecken des Update-Pakets

Sie können einen ePO-Server-Task erstellen, der Inhaltsupdate-Pakete automatisch in das ePO-Repository eincheckt, oder Sie können ein Update-Paket herunterladen und es manuell einchecken.

So fügen Sie Update-Pakete automatisch hinzu:

1 Wählen Sie den ePO-Servernamen in der ePO-Konsolenstruktur aus und klicken Sie auf die Registerkarte **Geplante Tasks**.

2 Klicken Sie auf **Task erstellen**.

3 Geben Sie im Fenster **Neuen Task konfigurieren** den Namen für den Task ein, beispielsweise **HIP-Inhaltsupdates**.

4 Wählen Sie in der Liste **Task-Typ** die Option **Repository-Pull** aus.

5 Wählen Sie in der Liste **Zeitplantyp** eine Häufigkeit aus.

6 Klicken Sie auf **Weiter**.

7 Wählen Sie das Quell-Repository (**McAfeeHttp** oder **McAfeeFtp**) und alle anderen verfügbaren Optionen aus.

8 Klicken Sie auf **Fertig stellen**.

Durch diesen Task wird das Inhaltsupdate-Paket direkt von McAfee heruntergeladen, und zwar mit der angegebenen Häufigkeit. Das Paket wird anschließend dem Repository hinzugefügt, worduch die Datenbank mit neuem Host Intrusion Prevention-Inhalt aktualisiert wird.

So fügen Sie Update-Pakete manuell hinzu:

1 Wählen Sie das Repository in der ePO-Konsolenstruktur aus und klicken Sie auf **Paket einchecken**.

2 Klicken Sie auf **Weiter** und wählen Sie **Produkte oder Aktualisierung**.

3 Klicken Sie auf **Weiter** und geben Sie den vollständigen Pfad für die Datei **PkgCatalog.z** ein.

4 Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.

Aktualisieren der Clients

Nachdem das Update-Paket in das Repository eingecheckt wurde, können Sie Updates an den Client senden, indem Sie entweder einen Update-Task ausführen oder einen Agenten-Aktivierungsaufruf senden. Ein Client kann auch Updates anfragen.

So führen Sie einen Update-Task aus:

1 Wählen Sie den Computer, eine Gruppe oder Site in der ePO-Konsolenstruktur aus, an den/die Sie die Inhaltspdates senden möchten, und wählen Sie die Registerkarte **Tasks** aus.

2 Wählen Sie im Kontextmenü die Option **Task planen** aus.

3 Geben Sie den Namen des Tasks ein, wählen Sie **ePolicy Orchestrator-Agentenaktualisierung** aus und klicken Sie auf **OK**.

4 Klicken Sie mit der rechten Maustaste auf den Task und wählen Sie **Task bearbeiten.**

5 Klicken Sie im Dialogfeld für den ePolicy Orchestrator Scheduler auf **Einstellungen**.

6 Wählen Sie im angezeigten Dialogfeld **HIP-Inhalt** aus und klicken Sie auf **OK.** (Diese Option ist nur verfügbar, wenn ein Inhaltspaket in das Repository eingecheckt wird.)

7 Klicken Sie im Dialogfeld **Scheduler** in ePolicy Orchestrator auf die Registerkarte **Zeitplan** und wählen Sie aus, dass der Task sofort ausgeführt werden soll.

8 Heben Sie auf der Registerkarte **Task** die Auswahl von **Übernehmen** auf und klicken Sie auf **Aktivieren**.

9 Klicken Sie auf **Anwenden** und anschließend auf **OK**.

So senden Sie einen Agenten-Aktivierungsaufruf:

1 Klicken Sie mit der rechten Maustaste auf die Site, die Gruppe oder den Computer in der ePO-Konsolenstruktur, an die/den Sie die Inhaltsupdates senden möchten, und wählen Sie **Agenten-Aktivierungsaufruf** aus.

2 Setzen Sie die Zufallsgenerierung auf 0 Minuten und klicken Sie auf **OK**.

Die Inhaltsupdates werden gesendet und auf den Client angewendet.

So lassen Sie einen Client eine Aktualisierung anfordern:

(Nur zutreffend, wenn das Symbol für einen ePO-Agenten in der Taskleiste angezeigt wird.)

- Klicken Sie mit der rechten Maustaste auf das ePO-Symbol in der Taskleiste und wählen Sie **Jetzt aktualisieren**.

  Das Dialogfeld **McAfee AutoUpdate-Status** wird geöffnet. Die Inhaltsupdates werden gesendet und auf den Client angewendet.

9 Host Intrusion Prevention-Client

Der Host Intrusion Prevention-Client kann auf Windows-, Solaris- und Linux-Plattformen installiert werden. Nur die Windows-Version des Client hat eine Schnittstelle, aber alle Versionen verfügen über eine Funktion zur Fehlerbehebung. In diesem Abschnitt werden die grundlegenden Funktionen jeder Client-Version beschrieben.

- *Windows-Client*
- *Solaris-Client*
- *Linux-Client*

Windows-Client

Über eine Client-Schnittstelle ist die direkte clientseitige Verwaltung des Host-Intrusion Prevention Windows-Client verfügbar. Zum Anzeigen der Client-Konsole klicken Sie in der Systemablage auf das Client-Symbol oder wählen Sie im Menü **Start** die Optionsfolge **Programme | McAfee | Host Intrusion Prevention**.

Wenn die Client-Konsole zum ersten Mal angezeigt wird, sind die meisten Optionen gesperrt. Wenn sich die Konsole im Sperrmodus befindet, können Sie lediglich die aktuellen Einstellungen anzeigen und manuell Client-Regeln erstellen, sofern die manuelle Erstellung von Client-Regeln in der Client-UI-Richtlinie aktiviert ist. Um alle Einstellungen in der Konsole vollständig steuern zu können, müssen Sie die Benutzeroberfläche mit einem Kennwort entsperren, das in der angewendeten Client-UI-Richtlinie erstellt wurde. Detaillierte Informationen zu den entsprechenden Einstellungen der Client-UI-Richtlinie erhalten Sie unter *Erstellen und Anwenden einer Client-UI-Richtlinie* auf Seite 114.

Symbol in Systemablage

Wenn die Symbole für Host Intrusion Prevention in der Systemablage angezeigt werden, erhalten Sie Zugriff auf die Client-Konsole und der Status des Client wird angezeigt.

Symbol	Host Intrusion Prevention-Status
	Arbeitet ordnungsgemäß
	Ein potentieller Angriff wurde erkannt
	Deaktiviert oder arbeitet nicht ordnungsgemäß

Es wird einige Sekunden lang eine Beschreibung des Status angezeigt, wenn Sie den Mauszeiger einige Sekunden lang auf dem Symbol platzieren. Klicken Sie mit der rechten Maustaste auf das Symbol, um das Kontextmenü aufzurufen:

Klicken Sie auf...	Aktion
Konfigurieren	Öffnen Sie die Host Intrusion Prevention-Client-Konsole.
Info...	Öffnen des Dialogfelds **Info zu Host Intrusion Prevention**, das die Versionsnummer und andere Produktinformationen anzeigt.

Wenn die Option **Deaktivieren von Funktionen über das Taskleistenmenü zulassen** auf den Client angewendet wird, sind einige oder alle der folgenden zusätzlichen Befehle verfügbar:

Klicken Sie auf...	Ziel
Einstellungen wiederherstellen	Aktivieren aller deaktivierten Funktionen. Nur verfügbar, wenn eine oder mehrere Funktionen deaktiviert wurden.
Alle deaktivieren	Deaktivieren der IPS-, Firewall- und Anwendungs-blockierfunktionen. Nur verfügbar, wenn alle Funktionen aktiviert sind.
IPS deaktivieren	Deaktivieren der IPS-Funktion. Dies umfasst sowohl die Host-IPS- als auch die Netzwerk-IPS-Funktionen. Nur verfügbar, wenn die Funktion aktiviert ist.
Firewall deaktivieren	Deaktivieren der Firewall-Funktion. Nur verfügbar, wenn die Funktion aktiviert ist.
Anwendungsblockierung deaktivieren	Deaktivieren der Anwendungsblockierfunktion. Dies umfasst sowohl die Anwendungerstellungsblockierung als auch die Anwendungs-Hook-Blockierung. Nur verfügbar, wenn die Funktion aktiviert ist.

Client-Konsole

Über die Client-Konsole von Host Intrusion Prevention können Sie auf verschiedene Konfigurationsoptionen zugreifen. Führen Sie die folgenden Schritte aus, um die Konsole zu öffnen:

- Doppelklicken Sie auf das Symbol in der Systemablage.
- Klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie **Konfigurieren**.
- Wählen Sie im Menü **Start** die Optionsfolge **Programme | McAfee | Host Intrusion Prevention.**

In der Konsole können Sie Informationen zu den Funktionen von Host Intrusion Prevention anzeigen und konfigurieren. Sie umfasst mehrere Registerkarten, die jeweils einer speziellen Funktion der Host Intrusion Prevention entsprechen. Einzelheiten finden Sie unter:

- *Registerkarte „IPS-Richtlinie“* auf Seite 153.
- *Firewall-Richtlinie, Registerkarte* auf Seite 155.
- *Anwendungsrichtlinie, Registerkarte* auf Seite 157.
- *Registerkarte „Blockierte Hosts“* auf Seite 159.
- *Registerkarte „Anwendungsschutz“* auf Seite 161.
- *Registerkarte „Aktivitätsprotokoll“* auf Seite 162.

Entsperren der Client-Benutzeroberfläche

Ein Administrator, der Host Intrusion Prevention mithilfe von ePolicy Orchestrator über den Fernzugriff verwaltet, kann einen Kennwortschutz für die Benutzeroberfläche festlegen, um unbeabsichtigte Änderungen zu verhindern. Mit einem zeitbasierten und computerspezifischen Kennwort kann ein Administrator temporär die Benutzeroberfläche entsperren und Änderungen vornehmen.

So entsperren Sie die Benutzeroberfläche von Host Intrusion Prevention:

1 Das Kennwort erhalten Sie vom zuständigen Administrator von Host Intrusion Prevention.

Einzelheiten über das Erstellen eines Kennworts finden Sie unter *Kennwörter einrichten* auf Seite 115.

2 Wählen Sie im Menü **Task** die Option **Sperrung der Benutzeroberfläche aufheben** aus.

Das Dialogfeld **Anmeldung** wird angezeigt.

3 Geben Sie das Kennwort ein und klicken Sie auf **OK**. Wenn es sich bei dem Kennwort um ein Administratorkennwort und nicht um ein zeitgesteuertes Kennwort handelt, wählen Sie das Kontrollkästchen **Administratorkennwort** aus, bevor Sie auf **OK** klicken.

Festlegen von Optionen

Die Client-Konsole von Host Intrusion Prevention ermöglicht den Zugriff auf einige Einstellungen, die von der Client-UI-Richtlinie zur Verfügung gestellt werden; außerdem ermöglicht sie Ihnen, sie für den einzelnen Client anzupassen.

So passen Sie Client-Optionen an:

1 Klicken Sie im Menü **Bearbeiten** auf **Optionen**.

Das Dialogfeld **Optionen** von Host Intrusion Prevention wird angezeigt.

2 Aktivieren und deaktivieren Sie die entsprechenden Optionen je nach Bedarf.

Wählen Sie...	Ziel
Popup-Warnung anzeigen	Im Falle eines Angriffs wird ein Dialogfeld mit einer Warnung angezeigt. Genauere Informationen dazu finden Sie unter *Warnungen*.
Ton ausgeben	Bei einem Angriff wird ein Ton ausgegeben.
Taskleistensymbol blinken lassen	Das Symbol wechselt zwischen dem Standard- und dem Angriffsstatus, wenn ein Angriff stattfindet.
Sniffer Capture erstellen, falls verfügbar	Es wird eine Sniffer Capture-Spalte zum Aktivitätsprotokoll hinzugefügt, um anzugeben, dass Intrusionspaketdaten protokolliert wurden. Speichern Sie diese Daten zur späteren Analyse in einer McAfee Sniffer.cap-Datei.
Taskleistensymbol anzeigen	Das Host Intrusion Prevention-Symbol wird in der Systemablage angezeigt.
Fehlerbericht	Das Dienstprogramm für den Software-Fehlerbericht ist aktiviert, um Fehler an McAfee zu senden. Genauere Informationen dazu finden Sie unter *Fehlerbericht*.

Fehlerbericht

Host Intrusion Prevention umfasst ein Fehlerbericht-Dienstprogramm, das Software-Ausfälle aufspürt und protokolliert. Wenn diese Option aktiviert ist, wird der Benutzer aufgefordert, die Daten des erkannten Problems an den technischen Support von McAfee weiterzuleiten, wo sie gegebenenfalls zum Öffnen eines Support-Falles verwendet werden können.

Um das Fehlerbericht-Dienstprogramm zu verwenden, muss ein Computer Zugriff auf das Internet und einen Webbrowser haben, für den Java Script aktiviert ist.

Wenn der Warnungs-Manager von McAfee in dem Netzwerk installiert ist, in dem ein Computer abgestürzt ist, wird der Netzwerkadministrator darüber informiert, dass ein Problem erkannt wurde. Der Netzwerkadministrator kann den Benutzer darüber unterrichten, welche Maßnahmen zur Behebung des Problems zu treffen sind.

Wenn das Dienstprogramm einen Fehler erkennt, wählt der Benutzer eine der folgenden Optionen aus:

- **Daten senden:** Mit dieser Option wird eine Verbindung zur Website des technischen Supports von McAfee hergestellt und die Daten werden gesendet.
- **Fehler ignorieren:** Es wird keine Verbindung hergestellt.

Wenn Daten an die Website des technischen Supports von McAfee gesendet werden, wird der Benutzer ggf. nach zusätzlichen Daten gefragt. Wenn das Problem eine bekannte Ursache hat, kann der Benutzer auf eine Webseite geleitet werden, auf der er Informationen über das Problem und dessen Behebung erhält.

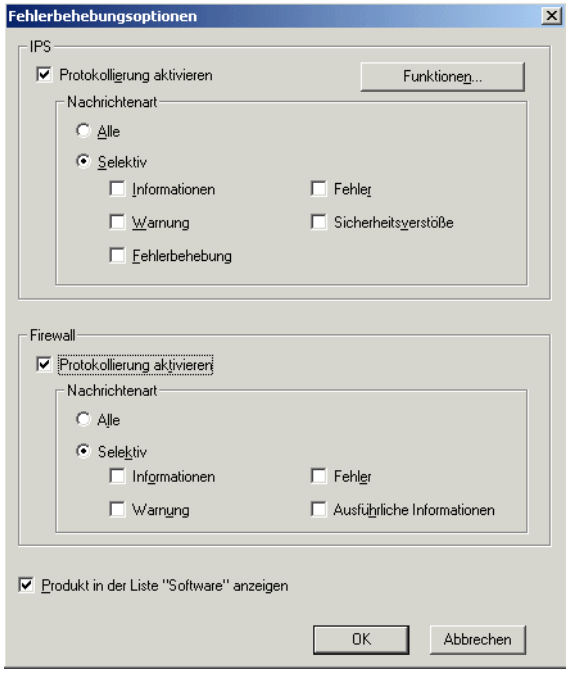
Fehlerbehebung

Host Intrusion Prevention enthält im Menü „Hilfe“ die Option **Fehlerbehebung**, die verfügbar ist, wenn die Benutzeroberfläche entsperrt ist. Zu den Optionen gehören das Aktivieren von IPS und die Firewall-Protokollierung sowie die Deaktivierung des Systemmoduls.

Protokollierung

Als Teil der Fehlerbehebung können Sie IPS- und Firewall-Aktivitätsprotokolle erstellen, die auf dem System analysiert oder an den Support von McAfee gesendet werden können, der Sie beim Beheben von Problemen unterstützen kann.

Abbildung 9-1 Fehlerbehebungsoptionen



So legen Sie die IPS-Protokollierungsoptionen fest:

1 Aktivieren Sie in IPS das Kontrollkästchen **Protokollierung aktivieren**.

2 Wählen Sie den Nachrichtentyp (**Alle** oder eine Kombination aus **Informationen**, **Warnung**, **Fehlerbehebung**, **Fehler** und **Sicherheitsverstöße) aus.**

   Sie müssen mindestens **Fehler** und **Sicherheitsverstöße** auswählen.

3 Klicken Sie auf **OK**.

   Die Informationen werden in der Datei `CSlog.txt` im Ordner `Programme\McAfee\Host Intrusion Prevention` gespeichert.

So legen Sie die Firewall-Protokollierungsoptionen fest:

1 Aktivieren Sie für die Firewall das Kontrollkästchen **Protokollierung aktivieren**.

2 Wählen Sie den Nachrichtentyp („Alle“ oder eine Kombination aus **Informationen**, **Warnung**, **Fehler** und **Kernel**) aus.

3 Klicken Sie auf **OK**.

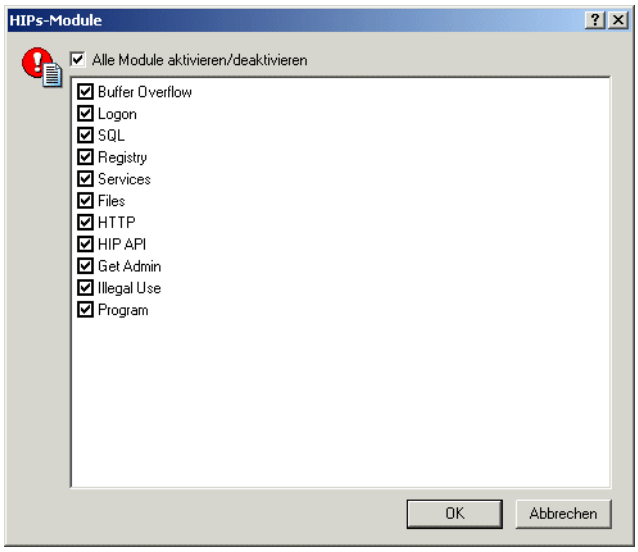
Die Informationen werden in der Datei `FireSvc.dbg` im Ordner `Programme\McAfee\Host Intrusion Prevention` gespeichert.

Host-IPS-Module

Bei der Fehlerbehebung können Sie auch Module deaktivieren, die einen Client schützen. McAfee empfiehlt, dass nur Administratoren, die mit dem McAfee-Support in Verbindung stehen, dieses Fehlerbehebungsverfahren verwenden.

Klicken Sie für den Zugriff auf **Funktion** im Dialogfeld **Fehlerbehebungsoptionen**. Deaktivieren Sie im Dialogfeld **HIPS-Module** ein oder mehrere Client-Systemmodule, indem Sie das Kontrollkästchen neben dem Modul auswählen. Nachdem das Problem behoben ist und Sie in die normale Betriebssystemumgebung zurückkehren, müssen alle Module ausgewählt sein.

Abbildung 9-2 HIPS-Module



Warnungen

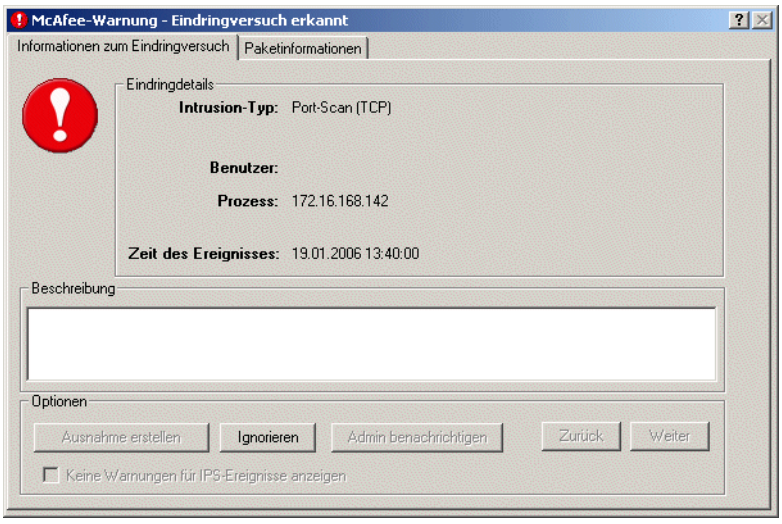
Einem Benutzer können mehrere Arten von Warnmeldungen angezeigt werden, auf die unterschiedlich reagiert werden muss. Dazu zählen Warnungen zu Intrusionserkennung, Firewall, Quarantäne, Anwendungsblockierung und Spoofing-Erkennung. Warnungen zur Firewall und zur Anwendungsblockierung werden nur angezeigt, wenn sich der Client für diese Funktionen im Lernmodus befindet.

Intrusionswarnungen

Wenn Sie den IPS-Schutz und die Option **Popup-Warnung anzeigen** aktivieren, wird diese Warnung automatisch angezeigt, wenn Host Intrusion Prevention einen potentiellen Angriff erkennt. Wenn sich der Client im adaptiven Modus befindet, wird diese Warnung nur dann angezeigt, wenn die Option **Client-Regeln zulassen** für die Signatur deaktiviert ist, die das Ereignis verursacht hat.

Auf der Registerkarte **Intrusionsinformationen** finden Sie Einzelheiten über den Angriff, der die Warnung generiert hat, einschließlich einer Beschreibung des Angriffs, des Benutzer-/Client-Computers, der das Ziel des Angriffs war, des am Angriff beteiligten Prozesses und der Zeit und des Datums des Abfangens durch Host Intrusion Prevention. Darüber hinaus kann eine generische, vom Administrator angegebene Meldung angezeigt werden.

Abbildung 9-3 Dialogfeld „Warnung für erkannte Intrusion“



Sie können das Ereignis entweder ignorieren, indem Sie auf **Ignorieren** klicken, oder Sie erstellen eine Ausnahmeregel für das Ereignis, indem Sie auf **Ausnahme erstellen** klicken. Die Schaltfläche **Ausnahme erstellen** ist nur aktiv, wenn die Option **Client-Regeln zulassen** für die Signatur aktiviert ist, die das Ereignis ausgelöst hat.

Wenn die Warnung das Ergebnis einer HIP-Signatur ist, wird in das Dialogfeld für die Ausnahmeregel vorab der Name des Prozesses, des Benutzers und der Signatur eingetragen. Sie können entweder **Alle Signaturen** oder **Alle Prozesse**, nicht jedoch beide Optionen auswählen. Der Benutzername wird immer in die Ausnahme aufgenommen.

Wenn die Warnung das Ergebnis einer NIP-Signatur ist, wird in das Dialogfeld für die Ausnahmeregel vorab der Name der Signatur und die Host-IP-Adresse eingetragen. Sie können optional **Alle Hosts** auswählen.

Darüber hinaus können Sie mit **Admin benachrichtigen** Informationen zum Ereignis an den Administrator von Host Intrusion Prevention senden. Diese Schaltfläche ist nur aktiv, wenn die Option **Dem Benutzer erlauben, den Administrator zu benachrichtigen** in der angewendeten **Client-UI**-Richtlinie aktiviert ist.

Wählen Sie die Option **Keine Warnungen für IPS-Ereignisse anzeigen**, um die Anzeige von Warnungen bei IPS-Ereignissen anzuhalten. Wenn Sie nach Auswahl dieser Option die Warnungen wieder anzeigen möchten, wählen Sie **Popup-Warnung anzeigen** im Dialogfeld **Optionen** aus.

Diese Intrusionswarnung wird auch bei Firewall-Intrusionen angezeigt, wenn eine Firewall-Regel gefunden wird, für die die Option **Regelübereinstimmung als Intrusion behandeln** ausgewählt ist.

Firewall-Warnungen

Wenn Sie den Firewall-Schutz und den **Lernmodus** für eingehenden oder ausgehenden Datenverkehr aktivieren, wird eine Firewall-Warnung angezeigt. Auf der Registerkarte **Anwendungsinformationen** werden Informationen zu der Anwendung angezeigt, die versucht, auf das Netzwerk zuzugreifen. Dies beinhaltet den Namen der Anwendung, den Pfad und die Version. Auf der Registerkarte **Verbindungsinformationen** werden Informationen zum Protokoll des Datenverkehrs, zur Adresse und den beteiligten Ports angezeigt.

So beantworten Sie Firewall-Warnungen des Lernmodus

1 Führen Sie auf der Registerkarte **Anwendungsinformationen** des Warnmeldungsdialogfelds einen der folgenden Schritte aus:

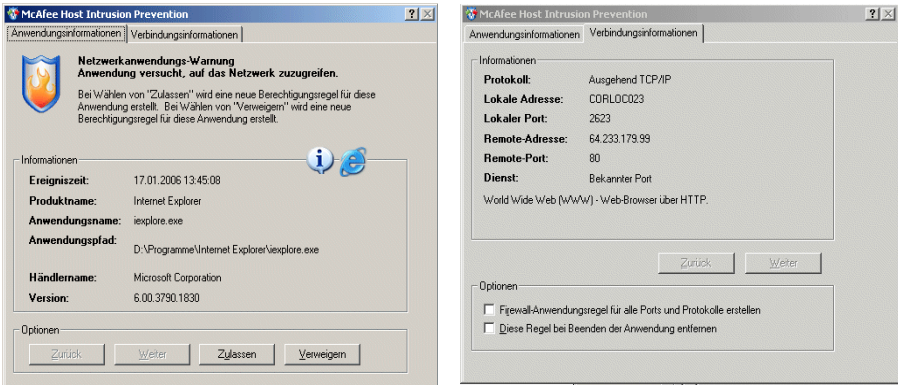
- Klicken Sie auf **Ablehnen**, um diesen und ähnlichen Datenverkehr zu blockieren.
- Klicken Sie auf **Zulassen**, um diesen und ähnlichen Datenverkehr zuzulassen.

2 Optional: Wählen Sie auf der Registerkarte **Verbindungsinformationen** die möglichen Optionen für die neue Firewall-Regel:

Wählen Sie...	Aktion
Firewall-Anwendungsregel für alle Ports und Dienste erstellen	Erstellt eine Regel, die den gesamten Datenverkehr einer Anwendung über alle Ports und Dienste zulässt bzw. blockiert. Wenn Sie diese Option nicht auswählen, dann gilt die neue Firewall-Regel nur für bestimmte Ports: ■ Wenn der abgefangene Datenverkehr einen Port unter 1.024 verwendet hat, dann bezieht sich die neue Regel nur auf diesen Port. ■ Wenn der Datenverkehr den Port 1.024 oder einen darüberliegenden verwendet hat, dann bezieht sich die neue Regel auf alle Ports zwischen 1.024 und 65.535.
Diese Regel nach Beenden der Anwendung löschen	Erstellt eine temporäre Regel, die beim Schließen der Anwendung gelöscht wird. Wenn Sie diese Option nicht auswählen, dann wird die neue Firewall-Regel als permanente Client-Regel erstellt.

Die Host Intrusion Prevention erstellt die neue Firewall-Regel auf der Grundlage der ausgewählten Optionen, fügt diese zur Liste der **Firewall-Regeln** hinzu und wendet sie automatisch auf ähnlichen Datenverkehr an.

Abbildung 9-4 Firewall-Warnung – Die Registerkarten „Anwendungsinformationen“ und „Verbindungsinformationen“



Anwendungsblockierwarnungen

Wenn in der Richtlinie **Anwendungsblockieroptionen** die Anwendungserstellung oder der Anwendungs-Hook aktiviert ist, überwacht Host Intrusion Prevention die Anwendungsaktivitäten und lässt diese auf der Grundlage der in der Richtlinie **Anwendungsblockierregeln** definierten Regeln zu oder blockiert sie.

Wenn der **Lernmodus** für die Erstellungsblockierung oder die Hook-Blockierung aktiviert ist, zeigt die Host Intrusion Prevention eine **Anwendungserstellungswarnung** oder eine **Anwendungs-Hook-Warnung** an, sobald versucht wird, eine unbekannte Anwendung auszuführen oder mit einem anderen Programm zu verbinden.

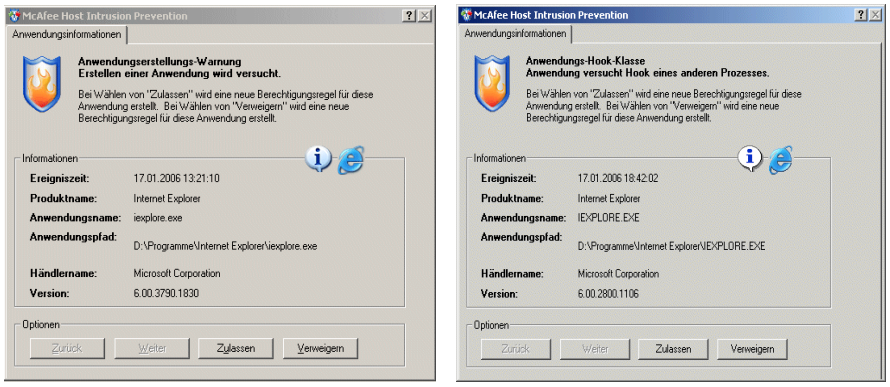
Auf der Registerkarte **Anwendungsinformationen** werden Informationen zur Anwendung angezeigt, die ausgeführt werden bzw. erstellt werden soll oder für die ein Hook mit einem anderen Prozess erstellt werden soll. Dies umfasst den Namen, den Pfad und die Version der Anwendung.

Verwenden Sie dieses Dialogfeld, um eine Aktion auszuwählen:

- Klicken Sie auf **Zulassen**, damit die Anwendung ihre Aktion abschließen kann:
  - Wenn Sie bei einer **Anwendungserstellungswarnung** auf **Zulassen** klicken, wird die Anwendung ausgeführt.
  - Wenn Sie bei einer **Anwendungs-Hook-Warnung** auf **Zulassen** klicken, verbindet sich die Anwendung mit einem anderen Programm.
- Klicken Sie auf **Ablehnen**, um die Anwendung zu blockieren:
  - Wenn Sie bei einer **Anwendungserstellungswarnung** auf **Ablehnen** klicken, wird das Ausführen der Anwendung verhindert.
  - Wenn Sie bei einer **Anwendungs-Hook-Warnung** auf **Ablehnen** klicken, wird verhindert, dass sich die Anwendung mit einem anderen Programm verbindet.

Wenn Sie auf **Zulassen** oder **Ablehnen** klicken, erstellt die Host Intrusion Prevention auf der Grundlage Ihrer Auswahl eine neue Anwendungsregel. Diese Regel wird nach dem Sammeln der Client-Eigenschaften zur Registerkarte **Anwendungs-Client-Regeln** der Richtlinie **Anwendungsregeln** hinzugefügt. Die Anwendung wird dann automatisch zugelassen oder blockiert.

Abbildung 9-5 Anwendungsblockierungswarnung bei Erstellung und Hooks

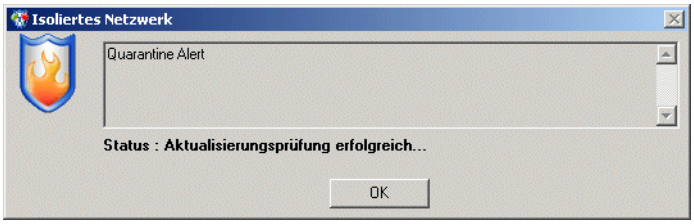


Quarantänewarnungen

Wenn Sie den Quarantänemodus aktivieren und die IP-Adresse des Client für die Quarantäneprüfung in der Richtlinie **Quarantäneoptionen** angeben, wird in folgenden Situationen eine Quarantänewarnung angezeigt:

- Ändern der IP-Adresse des Client-Computers.
- Trennen und erneutes Herstellen der Client-Ethernet-Verbindung.
- Neustarten des Client.

Abbildung 9-6 Quarantänewarnung



Warnungen bei erkanntem Spoofing

Wenn Sie die IPS-Funktion aktivieren, wird diese Warnung automatisch angezeigt, wenn Host Intrusion Prevention eine Anwendung auf dem Computer erkennt, die Spoof-Netzwerkdaten sendet. Das bedeutet, dass die Anwendung versucht, den Datenverkehr als von Ihrem Computer ausgehend zu tarnen; tatsächlich stammt er jedoch von einem anderen Computer. Hierzu ändert sie die IP-Adresse in den ausgehenden Paketen. Spoofing ist stets eine verdächtige Aktivität. Wenn dieses Dialogfeld angezeigt wird, sollten Sie sofort die Anwendung untersuchen, die den Spoof-Datenverkehr gesendet hat.

Das Dialogfeld **Warnungen bei erkanntem Spoofing** wird nur angezeigt, wenn Sie die Option **Popup-Warnung anzeigen** auswählen. Wenn Sie diese Option nicht aktivieren, blockiert Host Intrusion Prevention automatisch Spoof-Datenverkehr, ohne Sie diesbezüglich zu benachrichtigen.

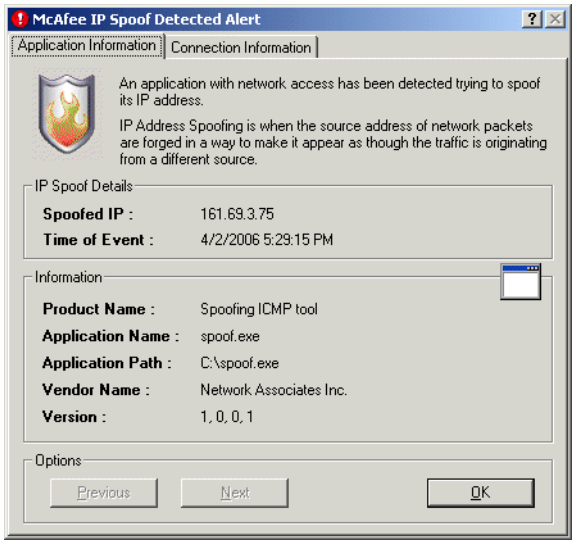
Das Dialogfeld **Warnung bei erkanntem Spoofing** entspricht weitgehend der Warnung durch die Firewall-Funktion **Lernmodus**. Es zeigt Informationen über abgefangenen Datenverkehr auf zwei Registerkarten an – auf der Registerkarte **Anwendungsinformationen** und auf der Registerkarte **Verbindungsinformationen**.

Auf der Registerkarte **Anwendungsinformationen** wird angezeigt:

- Die IP-Adresse, von der der Datenverkehr angeblich stammt.
- Informationen über das Programm, das den Spoof-Datenverkehr generiert hat.
- Das Datum und die Zeit des Abfangens des Datenverkehrs durch Host Intrusion Prevention.

Auf der Registerkarte **Verbindungsinformationen** werden weitere Netzwerkdaten angezeigt: Insbesondere die **Lokale Adresse** zeigt die IP-Adresse an, die die Anwendung angeblich hat, während die **Remote-Adresse** die tatsächliche IP-Adresse anzeigt.

Abbildung 9-7 Dialogfeld „Warnung bei erkanntem IP-Spoofing“

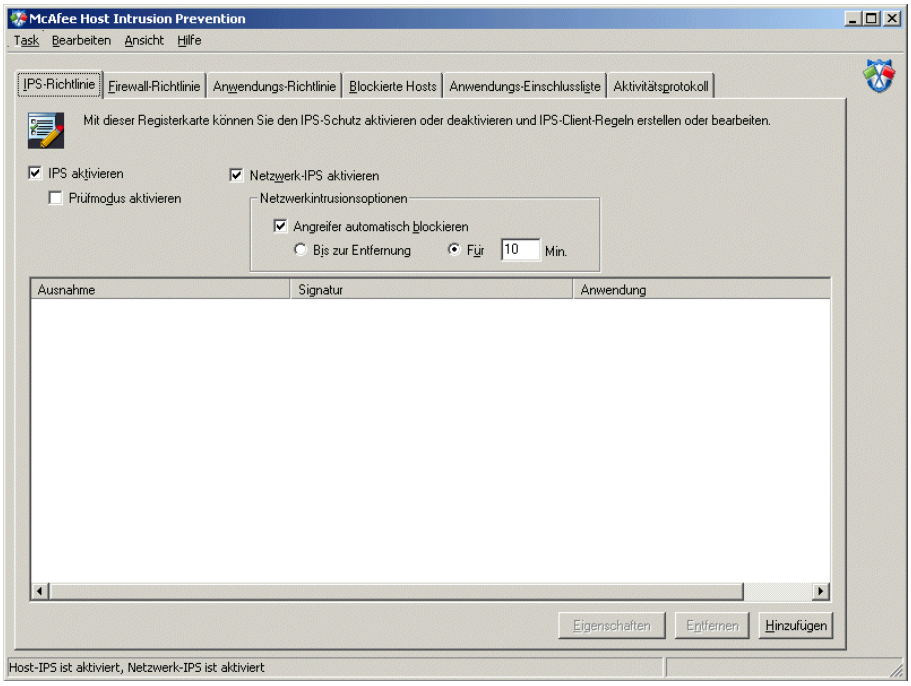

McAfee IP Spoof Detected Alert
Application Information
Connection Information
An application with network access has been detected trying to spoof its IP address.
IP Address Spoofing is when the source address of network packets are forged in a way to make it appear as though the traffic is originating from a different source.
IP Spoof Details
Spoofed IP : 161.69.3.75
Time of Event : 4/2/2006 5:29:15 PM
Information
Product Name : Spoofing ICMP tool
Application Name : spoof.exe
Application Path : C:\spoof.exe
Vendor Name : Network Associates Inc.
Version : 1, 0, 0, 1
Options
Previous
Next
OK

Wenn Host Intrusion Prevention Spoof-Netzwerkdatenverkehr erkennt, versucht sie, sowohl den Datenverkehr als auch die Anwendung zu blockieren, die ihn generiert hat. Hierzu fügt sie eine neue Regel am Ende der Liste der Firewall-Regeln hinzu. Die Regel **Spoofing-Angreifer blockieren** blockiert sämtlichen Datenverkehr, der von der verdächtigen Anwendung erstellt wurde; sofern sie nicht mit einer anderen Regel in der Liste überschrieben wird.

Registerkarte „IPS-Richtlinie“

Verwenden Sie die Registerkarte „IPS-Richtlinie“, um die IPS-Funktion zu konfigurieren, die einen Schutz vor Host-Intrusionsangriffen bietet, die auf Signatur- und Verhaltensregeln basieren. Über diese Registerkarte können Sie Funktionen aktivieren und deaktivieren und Client-Ausnahmeregeln konfigurieren. Weitere Einzelheiten über IPS-Richtlinien finden Sie unter *Kapitel 4, IPS-Richtlinien*.

Abbildung 9-8 Registerkarte „IPS-Richtlinie“



IPS-Richtlinienoptionen

Mit den Optionen oben auf der Registerkarte werden die Einstellungen gesteuert, die durch serverseitige IPS-Richtlinien zur Verfügung gestellt werden, nachdem die Client-Benutzeroberfläche entsperrt ist.

So passen Sie IPS-Richtlinienoptionen an:

1 Klicken Sie auf die Registerkarte **IPS-Richtlinie**.

2 Aktivieren und deaktivieren Sie die entsprechende Option je nach Bedarf.

Wählen Sie...	Ziel
Host-IPS aktivieren	Aktivieren des Schutzes durch Host Intrusion Prevention.
Netzwerk-IPS aktivieren	Aktivieren des Schutzes durch die Netzwerk-Intrusionsprävention.
Adaptiven Modus aktivieren	Aktivieren des Adaptiven Modus, um automatisch Ausnahmen für Intrusionspräventions-Signaturen zu erstellen.
Angreifer automatisch blockieren	Automatisches Blockieren von Netzwerkintrusions-Angriffen für einen bestimmten Zeitraum. Aktivieren Sie **Bis zur Entfernung**, um einen Angriff bis zum Entfernen zu blockieren, oder aktivieren Sie **für X Min.**, um einen Angriff für einen bestimmten Zeitraum zu blockieren (laut Standardeinstellung 30 Minuten).

IPS-Richtlinienausnahmeregeln

Die IPS-Ausnahmeregelliste zeigt Client-Ausnahmeregeln zum Anzeigen und Bearbeiten an.

So bearbeiten Sie Ausnahmeregeln:

1 Klicken Sie auf **Hinzufügen**, um eine Regel hinzuzufügen.

Das Dialogfeld **Ausnahmeregel** wird angezeigt.

2 Geben Sie eine Beschreibung für die Regel ein.

3 Wählen Sie in der Anwendungsliste die Anwendung aus, für die die Regel gilt, oder klicken Sie auf **Durchsuchen**, um nach der Anwendung zu suchen.

4 Wählen Sie **Ausnahmeregel ist aktiv**, um die Regel zu aktivieren.

Die Ausnahme gilt für alle Signaturen, ist laut Standardeinstellung nicht aktiviert und nicht ausgewählt; diese Option wendet die Ausnahme auf alle Signaturen an.

5 Klicken Sie auf **OK**.

Die neue Regel wird in der Liste angezeigt.

6 Führen Sie für andere Bearbeitungen einen der folgenden Schritte durch:

Ziel	Aktion...
Anzeigen der Einzelheiten einer Regel oder Bearbeiten einer Regel	Doppelklicken Sie auf eine Regel oder wählen Sie eine Regel aus und klicken Sie auf **Eigenschaften**. Das Dialogfeld **Ausnahmeregel** wird angezeigt, in dem Regelinformationen angezeigt werden, die bearbeitet werden können.
Aktivieren/ Deaktivieren einer Regel	Aktivieren oder Deaktivieren Sie das Kontrollkästchen **Ausnahmeregel ist aktiv** im Dialogfeld **Ausnahmeregel**. Sie können auch das Kontrollkästchen neben dem Regelsymbol in der Liste aktivieren oder deaktivieren.
Löschen von Regeln	Wählen Sie eine Regel aus und klicken Sie auf **Entfernen**.

Ausnahmeregelliste

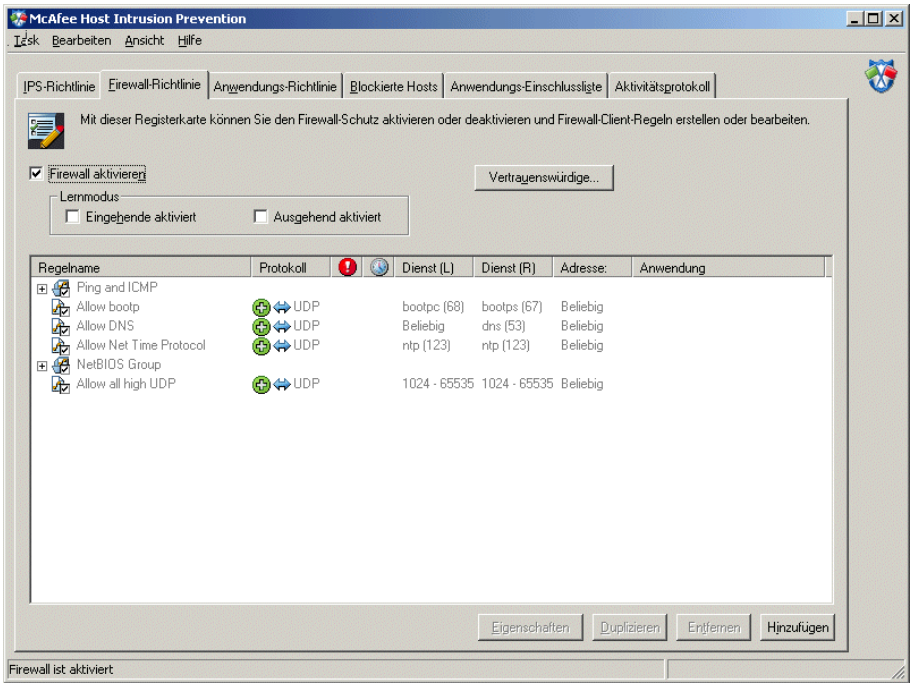
Die Ausnahmeregelliste zeigt Ausnahmeregeln, die für den Client relevant sind, mit zusammengefassten und detaillierten Informationen über jede Regel an.

Diese Spalte...	zeigt an
Ausnahme	Name der Ausnahme.
Signatur	Der Name der Signatur, für den die Ausnahme erstellt wird.
Anwendung	Die Anwendung, für die diese Regel gilt, einschließlich des Programmnamens und des Namens der ausführbaren Datei.

Firewall-Richtlinie, Registerkarte

Verwenden Sie die Registerkarte **Firewall-Richtlinie**, um die Firewall-Funktion zu konfigurieren, die basierend auf den von Ihnen definierten Regeln die Netzwerkkommunikation gestattet oder blockiert. Über diese Registerkarte können Sie Funktionen aktivieren und deaktivieren und Client-Firewall-Regeln konfigurieren. Weitere Einzelheiten über Firewall-Richtlinien finden Sie unter *Kapitel 5, Firewall-Richtlinien*.

Abbildung 9-9 Firewall-Richtlinie, Registerkarte



Optionen für „Firewall-Richtlinie“

Mit den Optionen oben auf der Registerkarte werden die Einstellungen gesteuert, die durch serverseitige Firewall-Richtlinien zur Verfügung gestellt werden.

So passen Sie die Optionen für „Firewall-Richtlinie“ an:

1 Klicken Sie auf die Registerkarte **IPS-Richtlinie**.

2 Aktivieren und deaktivieren Sie die entsprechende Option je nach Bedarf.

Wählen Sie...	Aktion
Firewall aktivieren	Aktivieren des Firewall-Richtlinienschutzes.
Lernmodus für Eingang aktiviert	Aktivieren des Lernmodus für eingehenden Datenverkehr.
Lernmodus für Ausgang aktiviert	Aktivieren des Lernmodus für ausgehenden Datenverkehr.
Vertrauenswürdig	Erstellen von vertrauenswürdigen Netzwerken. Genauere Informationen dazu finden Sie unter *Konfigurieren der Richtlinie „Vertrauenswürdige Netzwerke“* auf Seite 118.

Firewall-Richtlinienregeln

Die Liste mit den Firewall-Regeln zeigt Client-Regeln zum Anzeigen und Bearbeiten an. Einzelheiten über das Arbeiten mit Firewall-Regeln finden Sie unter.

- *Anzeigen und Bearbeiten von Firewall-Regeln* auf Seite 90.
- *Erstellen einer neuen Firewall-Regel oder Firewall-Gruppe* auf Seite 91.
- *Löschen einer Firewall-Regel oder -Gruppe* auf Seite 94.

Sie können keine Firewall-Verbindungsgruppen vom Client hinzufügen. Diese Funktion ist nur verfügbar in der Richtlinie „Firewall-Regeln“, die auf der ePolicy Orchestrator-Konsole verwaltet wird.

Firewall-Regelliste

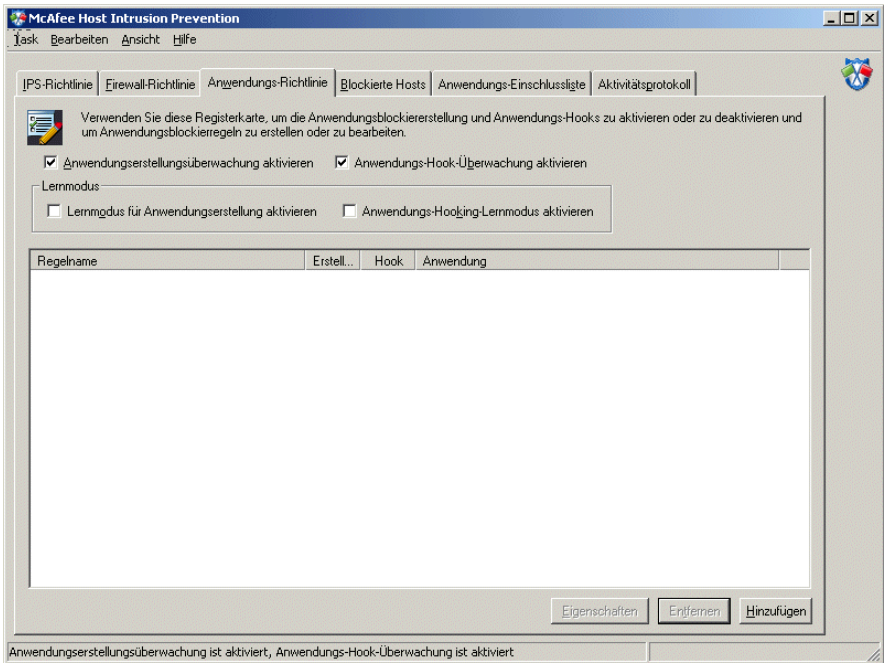
Die Firewall-Regelliste zeigt Regeln und Regelgruppen an, die für den Client relevant sind, mit zusammengefassten und detaillierten Informationen über jede Regel.

Diese Spalte...	Zeigt an
Beschreibung	Der Zweck dieser Regel oder Regelgruppe.
Protokoll	Das/die Protokoll(e), auf das/die die Regel angewendet wird/werden (TCP, UDP, ICMP). Ob es sich um eine Regel handelt, die den Datenverkehr gestattet oder blockiert: Gestattet Datenverkehr. Blockiert Datenverkehr. Ob die Regel auf eingehenden, ausgehenden Datenverkehr oder beides angewendet wird: Eingehender Datenverkehr. Ausgehenden Datenverkehr. Beide Richtungen.
	Ob Host Intrusion Prevention Datenverkehr, für den diese Regel zutrifft, auf dem System als Intrusion (oder Angriff) behandelt.
	Ob diese Regel nur zu bestimmten Zeiten angewendet wird.
Dienst (L)	Dienste auf Ihrem Computer, für die diese Regel gilt. Wenn möglich, werden in dieser Spalte die verknüpften Portnummern angezeigt. Sie können einen einzelnen Dienst festlegen, einen Dienstbereich, eine Liste von bestimmten Diensten oder alle (**Alle**) oder keine Dienste (**Nicht zutreffend**) festlegen.
Dienst (R)	Dienste auf dem Computer, an den Sie Datenverkehr senden oder von dem Sie Datenverkehr empfangen, für die diese Regel gilt. Wenn möglich, werden in dieser Spalte die verknüpften Portnummern angezeigt. Sie können einen einzelnen Dienst festlegen, einen Dienstbereich, eine Liste von bestimmten Diensten oder alle (**Alle**) oder keine Dienste (**Nicht zutreffend**) festlegen.
Adresse	Die IP-Adresse, das Subnetz, die Domäne oder eine andere bestimmte Bezeichnung, auf die diese Regel angewendet wird.
Anwendung	Die Anwendung, für die diese Regel gilt, einschließlich des Programmnamens und des Namens der ausführbaren Datei.

Anwendungsrichtlinie, Registerkarte

Verwenden Sie die Registerkarte **Anwendungsrichtlinie** zum Konfigurieren der Anwendungsblockierfunktion. Sie können festlegen, ob eine Anwendung ausgeführt werden kann (Anwendungserstellung) oder ob sie sich an andere Programme binden kann (Anwendungs-Hooking) und ob der Lernmodus und das Hooking für die Anwendungserstellung aktiviert werden können; außerdem können Sie Client-Anwendungsregeln konfigurieren. Weitere Einzelheiten über die Anwendungsblockierung finden Sie unter *Kapitel 6, Anwendungsblockierrichtlinien*.

Abbildung 9-10 Anwendungsrichtlinie, Registerkarte



Optionen für „Anwendungsrichtlinie“

Mit den Optionen oben auf der Registerkarte werden die Einstellungen gesteuert, die durch serverseitige Anwendungsrichtlinien zur Verfügung gestellt werden.

So passen Sie die Optionen für „Anwendungsrichtlinie“ an:

1 Klicken Sie auf die Registerkarte **Anwendungsrichtlinie**.

2 Aktivieren und deaktivieren Sie die entsprechende Option je nach Bedarf.

Wählen Sie...	Aktion
Anwendungs-erstellungs-blockierung aktivieren	Aktivieren der Blockierung von Anwendungserstellungen. Die Optionen für **Lernmodus für Anwendungserstellung aktivieren** werden aktiviert**.**
Blockierung für Anwendungs-Hooks aktivieren	Aktivieren der Blockierung für Anwendungs-Hooks. Die Option **Lernmodus für Anwendungs-Hooks aktivieren** wird aktiviert.
Lernmodus für Anwendungs-erstellung aktivieren	Aktivieren des Lernmodus für die Anwendungserstellung; der Benutzer wird dabei aufgefordert, die Anwendungserstellung zu gestatten oder zu blockieren.
Lernmodus für Anwendungs-Hooks aktivieren	Aktivieren des Lernmodus für Anwendungs-Hooks; der Benutzer wird dabei aufgefordert, Anwendungs-Hooks zuzulassen oder zu blockieren.

Regeln von „Anwendungsrichtlinie“

Die Liste der Anwendungsrichtlinienregeln zeigt Client-Regeln, die Sie aufrufen und bearbeiten können, an. Einzelheiten über das Arbeiten mit Anwendungsblockierregeln finden Sie unter.

- *Anzeigen und Bearbeiten von Anwendungsblockierregeln* auf Seite 106.
- *Erstellen neuer Anwendungsblockierregeln* auf Seite 107.
- *Löschen einer Anwendungsblockierregel* auf Seite 108.

Anwendungsregelliste

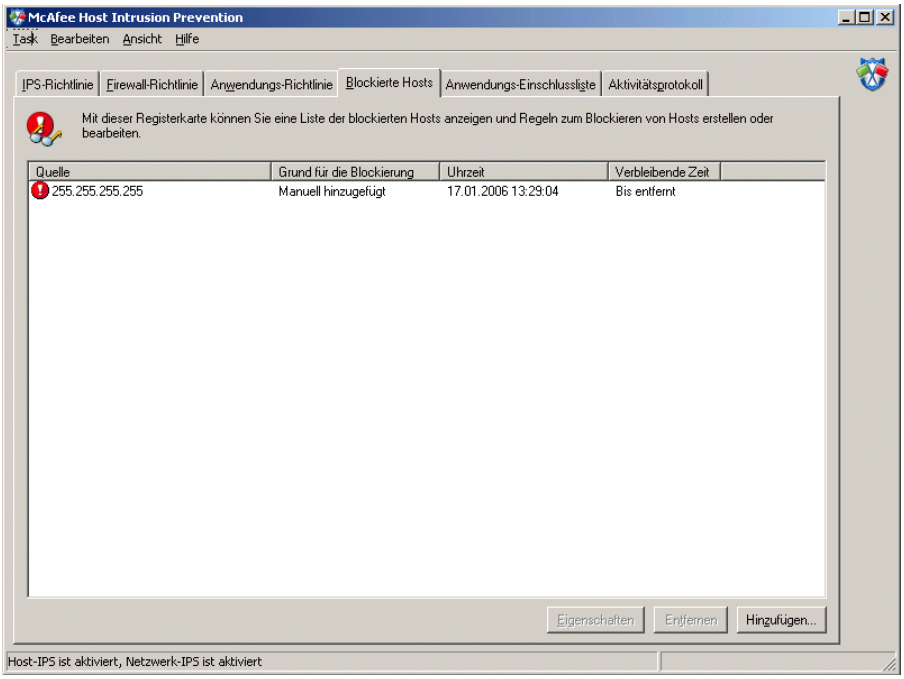
Die Anwendungsliste zeigt Regeln an, die für den Client relevant sind, mit zusammengefassten und detaillierten Informationen über jede Regel.

Diese Spalte...	zeigt an
Beschreibung	Der Zweck dieser Regel.
Erstellen	Ermöglicht die Ausführung der Anwendung. Blockiert die Ausführung der Anwendung.
Hook	Gestattet Anwendungen das Hooking an andere Programme. Blockiert das Hooking von Anwendungen an andere Programme.
Anwendung	Der Dateiname und der Pfad der Anwendung, auf die diese Regel angewendet wird.

Registerkarte „Blockierte Hosts“

Verwenden Sie die Registerkarte **Blockierte Hosts**, um eine Liste von blockierten *Hosts* (IP-Adressen) zu überwachen, die automatisch erstellt werden, wenn der Netzwerk-IPS-Schutz (NIPS) aktiviert ist (siehe *IPS-Richtlinienoptionen* auf Seite 153). Wenn die Option **Client-Regeln erstellen** in der Richtlinie „IPS-Optionen“ in der ePolicy Orchestrator-Konsole ausgewählt ist, können Sie die Liste der blockierten Hosts hinzufügen und bearbeiten.

Abbildung 9-11 Registerkarte „Blockierte Hosts“



Liste „Blockierte Hosts“

Sie können die Liste der blockierten Adressen anzeigen und bearbeiten. Bearbeitungsvorgänge beinhalten das Hinzufügen, Entfernen und Bearbeiten blockierter Hosts und das Anzeigen von Einzelheiten zu blockierten Hosts.

Die Liste der blockierten Hosts zeigt alle Hosts an, die gegenwärtig durch Host Intrusion Prevention blockiert werden. Jede Zeile stellt einen einzelnen Host dar. Weitere Informationen über einzelne Hosts finden Sie in den Informationen in den einzelnen Spalten.

Spalte	Anzeige
Quelle	■ Die durch Host Intrusion Prevention blockierte IP-Adresse.
Blockierungsgrund	■ Eine Erklärung, weshalb Host Intrusion Prevention diese Adresse blockiert hat. Wenn Host Intrusion Prevention diese Adresse der Liste hinzugefügt hat, weil ein Angriff auf das System versucht wurde, wird in dieser Spalte der Angriffstyp beschrieben. Wenn Host Intrusion Prevention diese Adresse hinzugefügt hat, weil eine der Firewall-Regeln die Option **Regelübereinstimmung als Intrusion behandeln** verwendet hat, wird in dieser Spalte der Name der relevanten Firewall-Regel aufgeführt. Wenn Sie diese Adresse manuell hinzugefügt haben, wird in dieser Spalte nur die von Ihnen blockierte IP-Adresse aufgeführt.
Uhrzeit	■ Zeit- und Datumsangabe über das Hinzufügen dieser Adresse zur Liste der blockierten Adressen.
Verbleibende Zeit	■ Dauer des Blockierens dieser Adresse durch Host Intrusion Prevention. Wenn Sie beim Blockieren der Adresse eine Ablaufzeit festgelegt haben, zeigt diese Spalte die verbleibende Minutenzahl bis zum Entfernen der Adresse aus der Liste durch Host Intrusion Prevention an. Wenn Sie angegeben haben, dass diese Adresse bis zum manuellen Entfernen aus der Liste blockiert bleiben soll, zeigt diese Spalte **Bis zur Entfernung** an.

So bearbeiten Sie die Liste „Blockierte Hosts“:

1 Klicken Sie auf **Hinzufügen**, um einen Host hinzuzufügen.

Das Dialogfeld **Blockierte Hosts** wird angezeigt.

2 Geben Sie die zu blockierende IP-Adresse ein. Um eine IPS-Adresse nach Domänenname zu suchen, klicken Sie auf **DNS Lookup**.

3 Legen Sie fest, wie lange die IP-Adresse blockiert werden soll:

- Wählen Sie **Bis zur Entfernung**, um den Host bis zum Löschen zu blockieren.
- Wählen Sie **Für** und geben Sie die Anzahl der Minuten bis 60 ein, um den Host für eine bestimmte Zeitspanne zu blockieren.

4 Klicken Sie auf **Quelle nachverfolgen**, um die IP-Adresse zurückzuverfolgen und Informationen zu sammeln, wie NetBIOS-Benutzer, MAC-Adresse, Telnet-Server-Banner, HTTP-Server-Banner, FTP-Server-Banner, SMTP-Server-Banner und DNS-Namen von nahen Adressen.

5 Klicken Sie auf **OK**.

Der neue blockierte Host wird in der Liste angezeigt.

Nachdem Sie eine blockierte Adresse erstellt haben, fügt Host Intrusion Prevention einen neuen Eintrag zur Liste auf der Registerkarte für den **Anwendungsschutz** hinzu. Sie blockiert jeglichen Kommunikationsversuch von dieser IP-Adresse, bis Sie die Adresse aus der Liste der blockierten Adressen entfernen oder bis eine festgelegte Zeitspanne verstrichen ist.

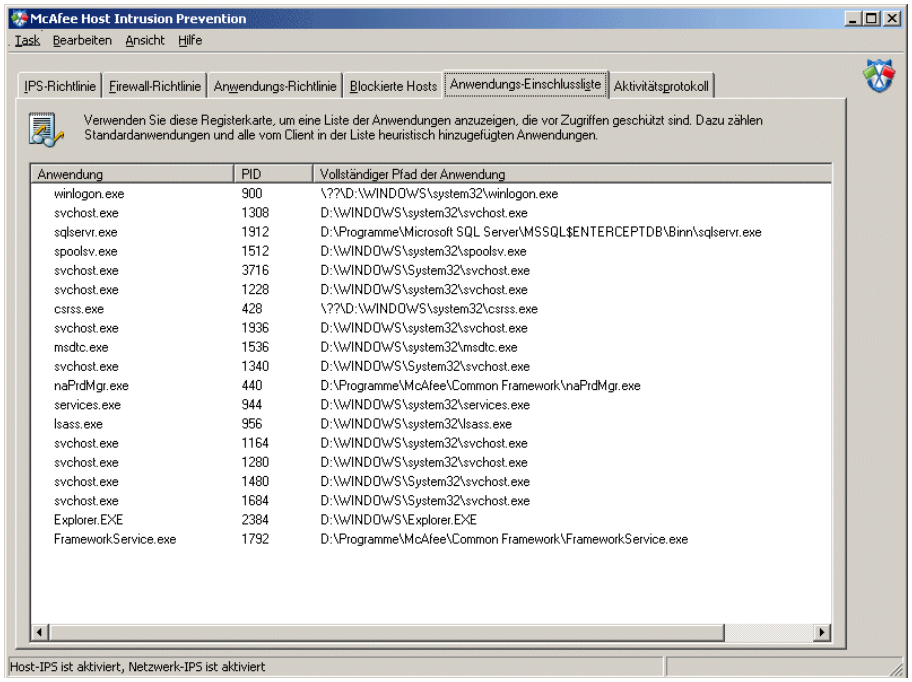
6 Führen Sie für andere Bearbeitungen einen der folgenden Schritte durch:

Ziel	Aktion...
Anzeigen der Einzelheiten oder Bearbeiten eines blockierten Hosts	Doppelklicken Sie auf einen Host-Eintrag oder wählen Sie einen Host aus und klicken Sie auf **Eigenschaften**. Im Dialogfeld **Blockierte Hosts** werden Informationen angezeigt, die bearbeitet werden können.
Löschen eines blockierten Hosts	Wählen Sie einen Host aus und klicken Sie auf **Entfernen**.

Registerkarte „Anwendungsschutz“

Auf der Registerkarte **Anwendungsschutz** wird eine Liste von geschützten Anwendungsprozessen auf dem Client angezeigt. Hierbei handelt es sich um eine über eine administrative Richtlinie erstellte schreibgeschützte Liste und um eine heuristisch erstellte clientspezifische Anwendungsliste. Genauere Informationen dazu finden Sie unter *Anwendungsschutzregeln* auf Seite 56.

Abbildung 9-12 Registerkarte „Anwendungsschutzliste“



Anwendungsschutzliste

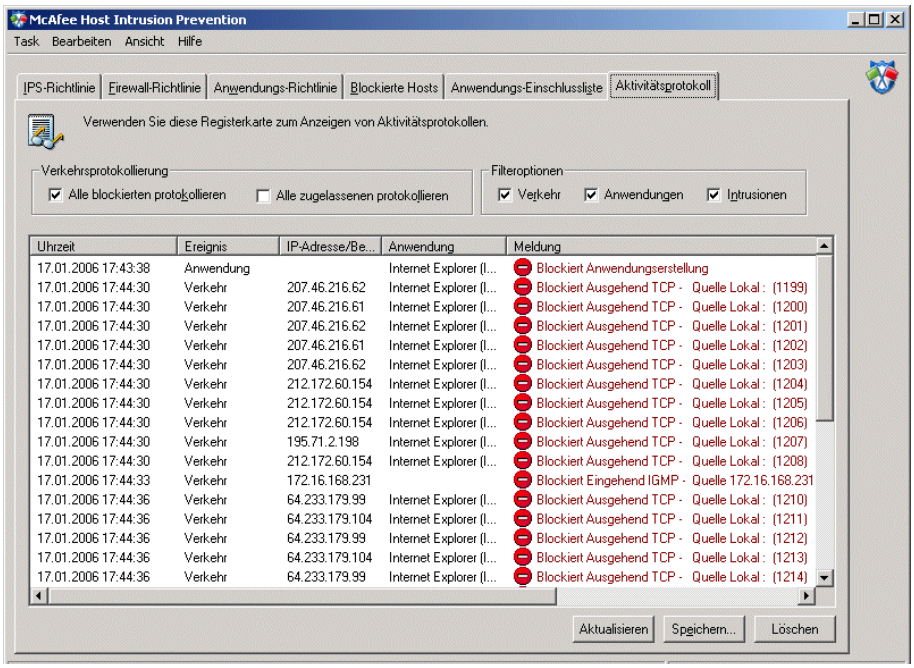
In dieser Liste werden alle überwachten Prozesse auf dem Client angezeigt.

Spalte	Anzeige
Prozess	Der Anwendungsprozess.
PID	Die Prozess-ID, die der Schlüssel für die Zwischenspeicher-Suche ist.
Vollständigen Pfad verarbeiten	Der vollständige Pfadname des Anwendungsprozesses.

Registerkarte „Aktivitätsprotokoll“

Verwenden Sie die Registerkarte **Aktivitätsprotokoll**, um die Protokollierungsfunktion zu konfigurieren und die Host Intrusion Prevention-Aktionen zurückzuverfolgen.

Abbildung 9-13 Registerkarte „Aktivitätsprotokoll“


McAfee Host Intrusion Prevention
Task Bearbeiten Ansicht Hilfe
IPS-Richtlinie
Firewall-Richtlinie
Anwendungs-Richtlinie
Blockierte Hosts
Anwendungs-Einschlussliste
Aktivitätsprotokoll
Verwenden Sie diese Registerkarte zum Anzeigen von Aktivitätsprotokollen.
Verkehrsprotokollierung
Alle blockierten protokollieren
Alle zugelassenen protokollieren
Filteroptionen
Verkehr
Anwendungen
Intrusionen
Uhrzeit
Ereignis
IP-Adresse/Be...
Anwendung
Meldung
17.01.2006 17:43:38 Anwendung Internet Explorer (I... Blockiert Anwendungserstellung
17.01.2006 17:44:30 Verkehr 207.46.216.62 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1199)
17.01.2006 17:44:30 Verkehr 207.46.216.61 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1200)
17.01.2006 17:44:30 Verkehr 207.46.216.62 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1201)
17.01.2006 17:44:30 Verkehr 207.46.216.61 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1202)
17.01.2006 17:44:30 Verkehr 207.46.216.62 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1203)
17.01.2006 17:44:30 Verkehr 212.172.60.154 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1204)
17.01.2006 17:44:30 Verkehr 212.172.60.154 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1205)
17.01.2006 17:44:30 Verkehr 212.172.60.154 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1206)
17.01.2006 17:44:30 Verkehr 195.71.2.198 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1207)
17.01.2006 17:44:30 Verkehr 212.172.60.154 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1208)
17.01.2006 17:44:33 Verkehr 172.16.168.231 Blockiert Eingehend IGMP - Quelle 172.16.168.231
17.01.2006 17:44:36 Verkehr 64.233.179.99 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1210)
17.01.2006 17:44:36 Verkehr 64.233.179.104 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1211)
17.01.2006 17:44:36 Verkehr 64.233.179.99 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1212)
17.01.2006 17:44:36 Verkehr 64.233.179.104 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1213)
17.01.2006 17:44:36 Verkehr 64.233.179.99 Internet Explorer (I... Blockiert Ausgehend TCP - Quelle Lokal : (1214)
Aktualisieren
Speichern...
Löschen

Optionen für „Aktivitätsprotokoll“

Mit den Optionen oben auf der Registerkarte werden die zu protokollierenden Elemente gesteuert und angezeigt.

So passen Sie die Optionen für „Aktivitätsprotokoll“ an:

1 Klicken Sie auf die Registerkarte **Aktivitätsprotokoll**.

2 Aktivieren und deaktivieren Sie die entsprechende Option je nach Bedarf.

Wählen Sie...	Aktion
Verkehrsprotokollierung – Alle Blockierungen protokollieren	Protokollieren des gesamten blockierten Firewall-Datenverkehrs.
Verkehrsprotokollierung – Alle Gestatteten protokollieren	Protokollieren des gesamten gestatteten Firewall-Datenverkehrs.
Filteroptionen – Verkehr	Filtern der Daten zum Anzeigen von blockiertem und gestattetem Firewall-Datenverkehr.
Filteroptionen – Anwendungen	Filtern der Daten zum Anzeigen von durch Anwendungen verursachten Ereignissen.
Filteroptionen – Intrusionen	Filtern der Daten zum Anzeigen von Intrusionen.

Sie können die Protokollierung für den Firewall-Datenverkehr aktivieren und deaktivieren, jedoch nicht für IPS oder Anwendungsblockierfunktionen. Sie können jedoch festlegen, dass diese Ereignisse im Protokoll durch Filtern ausgeblendet werden.

Liste „Aktivitätsprotokoll“

Das „Aktivitätsprotokoll“ enthält ein laufendes Aktivitätsprotokoll. Die neuesten Aktivitäten werden unten in der Liste angezeigt.

Spalte	Anzeige
Uhrzeit	Datum und Uhrzeit der Host Intrusion Prevention-Aktion.
Ereignis	Die Funktion, die diese Aktion durchgeführt hat. ■ **Verkehr** weist auf eine Firewall-Aktion hin. ■ **Anwendung** weist auf eine Anwendungsblockieraktion hin. ■ **Intrusion** weist auf eine IPS-Aktion hin. ■ **System** weist auf einen Ereignisbezug zu den internen Komponenten der Software hin. ■ **Dienst** weist auf einen Ereignisbezug zum Dienst oder den Treibern der Software hin.
Quelle	Die Remote-Adresse, an die diese Kommunikation entweder gesendet oder von der sie empfangen wurde.
Intrusionsdaten **Hinweis:** Diese Spalte wird nur angezeigt, wenn Sie die Option **Sniffer Capture bei Intrusion erstellen...** im **McAfee Host Intrusion Prevention-Optionen**-Dialogfeld ausgewählt haben.	Ein Symbol, das anzeigt, dass Host Intrusion Prevention die mit dem Angriff verknüpften Paketdaten gespeichert hat. (Dieses Symbol wird in den IPS-Protokolleinträgen angezeigt.) zeigt, dass Sie die mit diesem Protokolleintrag verknüpften Paketdaten exportieren können. Klicken Sie mit der rechten Maustaste auf den Protokolleintrag, um die Daten in einer Sniffer-Datei zu speichern.
Anwendung	Das Programm, das die Aktion verursacht hat.
Meldung	Eine Beschreibung der Aktion mit einem Höchstmaß an Einzelheiten.

Sie können diese Liste löschen, indem Sie die Protokollinhalte entfernen oder indem Sie sie in einer TXT-Datei speichern.

Ziel	Aktion...
Endgültiges Löschen der Protokollinhalte	Klicken Sie auf **Löschen**.
Speichern der Protokollinhalte und Löschen der Liste aus der Registerkarte	Klicken Sie auf **Speichern**. Benennen und speichern Sie die TXT-Datei im angezeigten Dialogfeld **Protokolldatei speichern unter**.

Solaris-Client

Der Host Intrusion Prevention 6.1 Solaris-Client erkennt und blockiert schädliche Angriffe, mit denen versucht wird, die Dateien und Anwendungen auf einem Solaris-Server zu schädigen. Der Client schützt das Betriebssystem des Servers sowie Apache- und Sun-Webserver, wobei verstärkt auf das Verhindern von Pufferüberlaufangriffen geachtet wird.

Richtlinienerzwingung mit dem Solaris-Client

Nicht alle Richtlinien, die einen Windows-Client schützen, stehen für den Solaris-Client zur Verfügung. Host Intrusion Prevention schützt also den Hostserver vor schädlichen Angriffen, bietet jedoch keinen Firewall-Schutz. Die gültigen Richtlinien sind hier aufgelistet.

Mit dieser Richtlinie...	Sind folgende Optionen verfügbar...
HIP 6.1 ALLGEMEIN:	
Client-UI	Das Tool zur Fehlerbehebung kann nur mit dem **Administrator-** oder einem **zeitbasierten Kennwort** verwendet werden.
Vertrauenswürdige Netzwerke	Keines
Vertrauenswürdige Anwendungen	Nur mit **Für IPS als vertrauenswürdig markieren** und **Neuer Prozessname** können vertrauenswürdige Anwendungen hinzugefügt werden.
HIP 6.1 IPS:	
IPS-Optionen	■ **HIPS aktivieren** ■ **Adaptiven Modus aktivieren** ■ **Bestehende Client-Regeln zurückhalten**
IPS-Schutz	Alles
IPS-Regeln	■ **Ausnahmeregeln** ■ **Signaturen** (nur standardmäßige und benutzerdefinierte HIPS-Regeln) **Hinweis:** NIPS-Signaturen und **Anwendungsschutzregeln** sind nicht verfügbar.
IPS-Ereignisse	Alles
IPS-Client-Regeln	Alles
IPS-Ausnahmeregeln suchen	Alles
HIP 6.1 FIREWALL	Keines
HIP 6.1 ANWENDUNGSBLOCKIERUNG	Keines

Problembehandlung

Nach dem Installieren und Starten des Solaris-Client schützt er seinen Host. Möglicherweise müssen Sie jedoch Probleme bei der Installation oder dem Betrieb des Client beheben.

Probleme bei der Installation des Client

Wenn während der Installation oder Deinstallation des Client ein Problem aufgetreten ist, können Sie es auf verschiedene Arten untersuchen. Sie können beispielsweise sicherstellen, dass alle erforderlichen Dateien im richtigen Verzeichnis installiert wurden, den Client deinstallieren und dann erneut installieren und die Prozessprotokolle überprüfen.

Überprüfen der Installationsdateien

Nach der Installation sollten Sie überprüfen, ob alle Dateien im richtigen Verzeichnis auf dem Client installiert wurden. Das Verzeichnis `opt/McAfee/hip` sollte die folgenden grundlegenden Dateien und Verzeichnisse enthalten:

Datei-/Verzeichnisname	Beschreibung
HipClient HipClient-bin	Solaris-Client
HipClientPolicy.xml	Richtlinienregeln
hipts hipts-bin	Fehlerbehebungstool
*.so	Gemeinsame Objektmodule von Host Intrusion Prevention und dem ePO-Agenten
Protokollverzeichnis	Enthält die folgenden Protokolldateien: HIPShield.log und HIPClient.log

Der Installationsverlauf wird in die Datei `/opt/McAfee/etc/hip-install.log` geschrieben. Lesen Sie in dieser Datei nach, wenn Sie Fragen zur Installation oder Entfernung des Host Intrusion Prevention-Client haben.

Überprüfen, ob der Client ausgeführt wird

Der Client kann ordnungsgemäß installiert sein und trotzdem können Probleme bei der Nutzung auftreten. Wenn beispielsweise der Client nicht in der ePO-Konsole angezeigt wird, überprüfen Sie mithilfe eines der folgenden Befehle, ob er ausgeführt wird:

- `/etc/rc2.d/SS99hip status`
- `ps -ef | grep hip`

Probleme bei der Nutzung des Client

Der Solaris-Client verfügt nicht über eine Benutzeroberfläche zur Behebung von Nutzungsproblemen. Er bietet jedoch ein Fehlerbehebungstool in der Befehlszeile, *hipts*, das sich im Verzeichnis /`opt/McAfee/hip` befindet. Um dieses Tool verwenden zu können, müssen Sie ein Host Intrusion Prevention-Client-Kennwort eingeben. Verwenden Sie das Standardkennwort, das Sie mit dem Client erhalten haben (abcde12345), oder senden Sie eine Client-UI-Richtlinie an den Client, die entweder ein Administratorkennwort oder ein zeitbasiertes Kennwort enthält, das mit der Richtlinie festgelegt wurde und verwenden Sie dieses Kennwort.

Verwenden Sie das Fehlerbehebungstool für Folgendes:

- Angeben der Protokollierungseinstellungen und des Modulstatus für den Client.
- Aktivieren und Deaktivieren der Nachrichtenprotokollierung.
- Aktivieren und Deaktivieren der Module.

Melden Sie sich als Root-Benutzer an und führen Sie die folgenden Befehle aus, um bei der Fehlerbehebung zu helfen:

Befehl	Aktion
hipts status	Abrufen des aktuellen Status des Client, der besagt, welcher Typ von Protokollierung aktiviert ist und welche Module ausgeführt werden.
hipts logging on	Aktivieren der Protokollierung bestimmter Nachrichtentypen.
hipts logging off	Deaktivieren der Protokollierung für alle Nachrichtentypen Die Protokollierung ist standardmäßig deaktiviert.
hipts message <Meldungsname>:on	Anzeigen des angegebenen Nachrichtentyps, wenn die Protokollierung auf „on“ gesetzt ist Die Meldungen umfassen Folgendes: ■ error ■ warning ■ debug ■ info ■ violations
hipts message <Meldungsname>:off	Verbergen des angegebenen Nachrichtentyps, wenn die Protokollierung auf „on“ gesetzt ist. Fehlermeldungen sind standardmäßig deaktiviert.
hipts message all:on	Anzeigen aller Nachrichtentypen, wenn die Protokollierung auf „on“ gesetzt ist.
hipts message all:off	Verbergen aller Nachrichtentypen, wenn die Protokollierung auf „on“ gesetzt ist.
hipts engines <Modulname>:on	Aktivieren des angegebenen Moduls Das Modul ist standardmäßig aktiviert. Die Module umfassen: ■ MISC ■ FILES ■ GUID ■ MMAP ■ BO ■ ENV ■ HTTP
hipts engines <Modulname>:off	Deaktivieren des angegebenen Moduls.
hipts engines all:on	Aktivieren aller Module.
hipts engines all:off	Deaktivieren aller Module.

Zusätzlich zur Verwendung des Fehlerbehebungstools können Sie mithilfe der Dateien HIPShield.log und HIPClient.log im Verzeichnis `/opt/McAfee/hip/log` Vorgänge überprüfen oder Probleme nachverfolgen.

Starten und Anhalten des Client

Möglicherweise müssen Sie einen ausgeführten Client anhalten und ihn als Teil der Fehlerbehebung neu starten.

So halten Sie einen Solaris-Client an:

1 Deaktivieren Sie den IPS-Schutz. Verwenden Sie eine der folgenden Vorgehensweisen:

- Stellen Sie die **IPS-Optionen** in der ePO-Konsole auf **Aus** und wenden Sie die Richtlinie auf den Client an.
- Führen Sie folgenden Befehl aus: `hipts engines MISC:off.`

2 Führen Sie folgenden Befehl aus: `/etc/rc2.d/S99hip stop.`

So starten Sie einen Solaris-Client neu:

1 Führen Sie folgenden Befehl aus: `/etc/rc2.d/S99hip restart.`

2 Aktivieren Sie den IPS-Schutz. Verwenden Sie eine der folgenden Vorgehensweisen, je nachdem, welche Sie zum Anhalten des Client verwendet haben:

- Stellen Sie die **IPS-Optionen** in der ePO-Konsole auf **Ein** und wenden Sie die Richtlinie auf den Client an.
- Führen Sie folgenden Befehl aus: `hipts engines MISC:on.`

Linux-Client

Der Host Intrusion Prevention 6.1 Linux-Client erkennt und blockiert schädliche Angriffe, mit denen versucht wird, die Dateien und Anwendungen auf einem Linux-Server zu schädigen. Er nutzt den nativen SELinux-Schutzmechanismus und übersetzt IPS-Richtlinien in SELinux-Regeln und SELinux-Ereignisse zurück in IPS-Ereignisse und bietet außerdem eine einfache Verwaltungsmöglichkeit über die ePO-Konsole.

Richtlinienerzwingung mit dem Linux-Client

Nicht alle Richtlinien, die einen Windows-Client schützen, stehen für den Linux-Client zur Verfügung. Host Intrusion Prevention schützt also den Hostserver vor schädlichen Angriffen, bietet jedoch keinen Schutz vor Netzwerkintrusionen, einschließlich Pufferüberlauf. Die gültigen Richtlinien sind im Anschluss aufgeführt.

Mit dieser Richtlinie...	Sind folgende Optionen verfügbar...
HIP 6.1 ALLGEMEIN:	
Client-UI	Das Tool zur Fehlerbehebung kann nur mit dem **Administrator-** oder einem **zeitbasierten Kennwort** verwendet werden**.**
Vertrauenswürdige Netzwerke	Keines
Vertrauenswürdige Anwendungen	Nur mit **Für IPS als vertrauenswürdig markieren** und **Neuer Prozessname** können vertrauenswürdige Anwendungen hinzugefügt werden**.**
HIP 6.1 IPS:	
IPS-Optionen	■ **HIPS aktivieren** ■ **Adaptiven Modus aktivieren** ■ **Bestehende Client-Regeln zurückhalten**

Mit dieser Richtlinie...	Sind folgende Optionen verfügbar...
IPS-Schutz	Alles
IPS-Regeln	■ **Ausnahmeregeln** ■ **Signaturen** (nur standardmäßige und benutzerdefinierte HIPS-Regeln) **Hinweis:** NIPS-Signaturen und **Anwendungsschutzregeln** sind nicht verfügbar.
IPS-Ereignisse	Alles
IPS-Client-Regeln	Alles
IPS-Ausnahmeregeln suchen	Alles
HIP 6.1 FIREWALL	Keines
HIP 6.1 ANWENDUNGSBLOCKIERUNG	Keines

Anmerkungen zum Linux-Client

- Wenn Sie derzeit eine SELinux-Richtlinie oder standardmäßige Schutzeinstellungen verwenden, wird durch die Installation des Linux-Client die Richtlinie durch eine standardmäßige McAfee Host Intrusion Prevention-Richtlinie ersetzt. Durch die Deinstallation des Linux-Client wird die vorhergehende SELinux-Richtlinie wiederhergestellt.
- Der Linux-Client erfordert, dass SELinux installiert und aktiviert ist (eingestellt auf „enforce“ oder „permissive“). Wenn SELinux installiert aber deaktiviert ist, sollten Sie es aktivieren, es auf die gewünschte Richtlinie einstellen und den Computer neu starten, bevor Sie den Linux-Client installieren.
- Linux steuert Änderungen an den Dateiattributen mit einer einzigen SELinux-Berechtigung (file:setattr). SELinux kann chdir oder symlink nicht individuell steuern, es steuert keine Änderungen an Verzeichnissen oder das Erstellen eines Symbol-Links.
- SELinux verwendet einen obligatorischen Zugriffssteuerungsmechanismus, der mithilfe des Linux Security Modules (LSM)-Framework in den Linux-Kernel implementiert ist. Dieses Framework prüft auf zulässige Vorgänge, nachdem die standardmäßigen Linux-Zugriffskontrollen geprüft wurden. Da der Linux-Client LSM verwendet, funktioniert keine andere Anwendung, die LSM verwendet, solange die Stapelungsfunktion nicht implementiert ist.

Fehlerbehebung

Nach dem Installieren und Starten des Linux-Client schützt er seinen Host. Möglicherweise müssen Sie jedoch Probleme bei der Installation oder dem Betrieb des Client beheben.

Probleme bei der Installation des Client

Wenn während der Installation oder Deinstallation des Client ein Problem aufgetreten ist, können Sie es auf verschiedene Arten untersuchen. Sie können beispielsweise sicherstellen, dass alle erforderlichen Dateien im richtigen Verzeichnis installiert wurden, den Client deinstallieren und dann erneut installieren und die Prozessprotokolle überprüfen.

Überprüfen der Installationsdateien

Nach der Installation sollten Sie überprüfen, ob alle Dateien im richtigen Verzeichnis auf dem Client installiert wurden. Das Verzeichnis `opt/McAfee/hip` sollte die folgenden grundlegenden Dateien und Verzeichnisse enthalten:

Dateiname	Beschreibung
HipClient HipClient-bin	Linux-Client
HipClientPolicy.xml	Richtlinienregeln
hipts hipts-bin	Fehlerbehebungstool
*.so	Gemeinsame Objektmodule von Host Intrusion Prevention und dem ePO-Agenten
Protokollverzeichnis	Enthält die folgenden Protokolldateien: HIPShield.log und HIPClient.log

Der Installationsverlauf wird in die Datei `/opt/McAfee/etc/hip-install.log` geschrieben. Lesen Sie in dieser Datei nach, wenn Sie Fragen zur Installation oder Entfernung des Host Intrusion Prevention-Client haben.

Überprüfen, ob der Client ausgeführt wird

Wenn beispielsweise der Client in der ePO-Konsole nicht angezeigt wird, überprüfen Sie, ob der Client ausgeführt wird. Führen Sie hierzu den folgenden Befehl aus:

```
ps –ef | grep hip
```

Probleme bei der Nutzung des Client

Der Client kann ordnungsgemäß installiert sein und trotzdem können Probleme bei der Nutzung auftreten. Sie können prüfen, ob der Client ausgeführt wird, den Client anhalten und neu starten.

Fehlerbehebungstool

Der Linux-Client verfügt nicht über eine Benutzeroberfläche zur Behebung von Nutzungsproblemen. Er bietet jedoch ein Fehlerbehebungstool in der Befehlszeile, *hipts*, das sich im Verzeichnis `opt/McAfee/hip` befindet. Um dieses Tool verwenden zu können, müssen Sie ein Host Intrusion Prevention-Client-Kennwort eingeben. Verwenden Sie das Standardkennwort, das Sie mit dem Client erhalten haben (abcde12345), oder senden Sie eine Client-UI-Richtlinie an den Client, die entweder ein Administratorkennwort oder ein zeitbasiertes Kennwort enthält, das mit der Richtlinie festgelegt wurde, und verwenden Sie dieses Kennwort.

Verwenden Sie das Fehlerbehebungstool für Folgendes:

- Angeben der Protokollierungseinstellungen und des Modulstatus für den Client.
- Aktivieren und Deaktivieren der Nachrichtenprotokollierung.
- Aktivieren und Deaktivieren der Module.

Melden Sie sich als Root-Benutzer an und führen Sie die folgenden Befehle aus, um bei der Fehlerbehebung zu helfen.

Befehl	Aktion
hipts status	Abrufen des aktuellen Status des Client, der besagt, welcher Typ von Protokollierung aktiviert ist und welche Module ausgeführt werden.
hipts logging on	Aktivieren der Protokollierung bestimmter Nachrichtentypen.
hipts logging off	Deaktivieren der Protokollierung für alle Nachrichtentypen Die Protokollierung ist standardmäßig deaktiviert.
hipts message <Meldungsname>:on	Anzeigen des angegebenen Nachrichtentyps, wenn die Protokollierung auf „on“ gesetzt ist Die Meldungen umfassen Folgendes: ■ error ■ warning ■ debug ■ info ■ violations
hipts message <Meldungsname>:off	Verbergen des angegebenen Nachrichtentyps, wenn die Protokollierung auf „on“ gesetzt ist. Fehlermeldungen sind standardmäßig deaktiviert.
hipts message all:on	Anzeigen aller Nachrichtentypen, wenn die Protokollierung auf „on“ gesetzt ist.
hipts message all:off	Verbergen aller Nachrichtentypen, wenn die Protokollierung auf „on“ gesetzt ist.
hipts engines <Modulname>:on	Aktivieren des angegebenen Moduls Das Modul ist standardmäßig aktiviert. Die Module umfassen: ■ MISC ■ FILES
hipts engines <Modulname>:off	Deaktivieren des angegebenen Moduls.
hipts engines all:on	Aktivieren aller Module.
hipts engines all:off	Deaktivieren aller Module.

Zusätzlich zur Verwendung des Fehlerbehebungstools können Sie mithilfe der Dateien HIPShield.log und HIPClient.log im Verzeichnis McAfee/hip/log Vorgänge überprüfen oder Probleme nachverfolgen.

Starten und Anhalten des Client

Möglicherweise müssen Sie einen ausgeführten Client anhalten und ihn als Teil der Fehlerbehebung neu starten.

So halten Sie einen Linux-Client an:

1 Deaktivieren Sie den IPS-Schutz. Verwenden Sie eine der folgenden Vorgehensweisen:

- Stellen Sie die **IPS-Optionen** in der ePO-Konsole auf **Aus** und wenden Sie die Richtlinie auf den Client an.
- Führen Sie folgenden Befehl aus: `hipts engines MISC:off.`

2 Führen Sie folgenden Befehl aus: `hipts agent off.`

So starten Sie einen Linux-Client neu:

1 Führen Sie folgenden Befehl aus: `hipts agent on.`

2 Aktivieren Sie den IPS-Schutz. Verwenden Sie eine der folgenden Vorgehensweisen, je nachdem, welche Sie zum Anhalten des Client verwendet haben:

- Stellen Sie die **IPS-Optionen** in der ePO-Konsole auf **Ein** und wenden Sie die Richtlinie auf den Client an.
- Führen Sie folgenden Befehl aus: `hipts engines MISC:on.`

10 Häufig gestellte Fragen (FAQ)

In diesem Abschnitt werden einige in der Praxis auftauchende Fragen beantwortet, die im Zusammenhang mit der Verwendung von Host Intrusion Prevention 6.0 aufkommen können.

- *Was ist eine Richtlinie?*
- *Was ist die McAfee-Standardrichtlinie?*
- *Was passiert mit den Knoten des Verzeichnisses unter einem Knoten, dem ich eine neue Richtlinie zugewiesen habe?*
- *Welche Auswirkungen hat es auf die Knoten, auf die eine Richtlinie angewendet wird, wenn die Richtlinie geändert wird?*
- *Warum wird die neue Host Intrusion Prevention-Richtlinie, die ich zugewiesen habe, nicht durchgesetzt?*
- *Kann ich die Verwaltung von IPS- und Firewall-Richtlinien an verschiedene Verwalter delegieren, die sich an unterschiedlichen geografischen Standorten befinden?*
- *Kann ich dieselbe Sicherheitskonfiguration auf verschiedene Systeme anwenden?*
- *Kann ich die auf einen bestimmten Knoten oder Clients anwendbaren Richtlinien anzeigen oder bearbeiten?*
- *Wie kann ich alle verfügbaren Richtlinien und die Knoten anzeigen, denen diese zugewiesen sind?*
- *Wie kann ich die durch Clients ausgelösten IPS-Ereignisse anzeigen?*
- *Wie erstelle ich eine auf einem IPS-Ereignis basierende Ausnahme?*
- *Wie kann ich die IPS-Regelrichtlinien mithilfe des automatischen Tuning-Mechanismus verfeinern?*
- *Wie erstelle ich benutzerdefinierte Signaturen für eine IPS-Richtlinie?*
- *Wie reorganisiere ich vorhandene Ausnahmen und benutzerdefinierte Signaturen in einer neuen Richtlinie?*
- *Wie finde ich vorhandene Richtlinien, die mit einem bestimmten Profil übereinstimmen?*

Was ist eine Richtlinie?

Eine Richtlinie ist eine benutzerdefinierte Untermenge der Produkteinstellungen, die einer Richtlinienkategorie entspricht. Sie können beliebig viele benannte Richtlinien für jede Richtlinienkategorie erstellen, ändern oder löschen.

Was ist die McAfee-Standardrichtlinie?

Nach der Installation enthält jede Richtlinienkategorie mindestens eine benannte Richtlinie, McAfee-Standard. Die McAfee-Standardrichtlinien können weder bearbeitet noch umbenannt oder gelöscht werden.

Was passiert mit den Knoten des Verzeichnisses unter einem Knoten, dem ich eine neue Richtlinie zugewiesen habe?

Alle Knoten, für die für eine bestimmte Richtlinienkategorie die Vererbung aktiviert ist, erben die auf den übergeordneten Knoten angewendeten Richtlinien.

Welche Auswirkungen hat es auf die Knoten, auf die eine Richtlinie angewendet wird, wenn die Richtlinie geändert wird?

Alle Knoten, auf die eine Richtlinie angewendet wird, erhalten bei der nächsten Kommunikation zwischen Agent und Server oder bei Ausführung einer Agenten-Reaktivierung sämtliche an der Richtlinie vorgenommenen Änderungen. Die Richtlinie wird dann bei jedem Richtliniendurchsetzungsintervall erzwungen.

Warum wird die neue Host Intrusion Prevention-Richtlinie, die ich zugewiesen habe, nicht durchgesetzt?

Neue Richtlinienzuweisungen werden erst durchgesetzt, wenn nach der Zuweisung die nächste Kommunikation zwischen dem Agenten und dem Server stattfindet, oder bei Ausführung einer Agenten-Reaktivierung. Wenn die Client-UI mit einem Kennwort entsperrt wird, werden ebenfalls keine neuen Richtlinienzuweisungen erzwungen.

Kann ich die Verwaltung von IPS- und Firewall-Richtlinien an verschiedene Verwalter delegieren, die sich an unterschiedlichen geografischen Standorten befinden?

Ja. Host Intrusion Prevention bietet Ihnen die Möglichkeit, die Verantwortung für alle oder für einzelne Produktfunktionen, wie IPS oder Firewall, zu delegieren. Eine stärkere Verfeinerung der Rollen innerhalb der Funktion wird nicht unterstützt – beispielsweise die Client-Verwaltung und das Erstellen von Ausnahmen.

Weisen Sie Benutzerberechtigungen auf Site-Ebene zu, eine Ebene unter dem Stammverzeichnis, dann werden die Berechtigungen an alle unter der Site liegenden Knoten übergeben. Ausdrückliche Benutzerberechtigungen auf Knoten unterhalb der Site-Ebene werden nicht unterstützt. Um die Verwaltung nach geografischem Standort zu delegieren, legen Sie einen geografischen Standort an einem Site-Knoten fest und wenden dann die entsprechenden Benutzerrechte an.

Kann ich dieselbe Sicherheitskonfiguration auf verschiedene Systeme anwenden?

Knoten sind in der Konsolenstruktur hierarchisch angeordnet. Sie weisen Richtlinien Knoten zu, daher weisen die Knoten auf Site-Ebene in der Regel profilbasierte Gruppierungen auf, wie „Alle Server“, „Alle Desktops“, „IIS-Server“ oder „SQL-Server“. Dieses Gruppierungsmuster kann unter allen Site-Knoten repliziert werden.

ePolicy Orchestrator ermöglicht das Erstellen von knotenunabhängigen Richtlinien, die von allen Knoten gemeinsam verwendet werden können. Wenn Sie einem Knoten eine Richtlinie zuweisen, wird diese von den untergeordneten Knoten automatisch übernommen, sofern sie nicht mit einer anderen Richtlinie überschrieben wird. Sie können eine Richtlinie erstellen, die zu einem Profil passt, wie eine IIS-Server-Richtlinie, und diese auf alle entsprechenden Knotengruppen, wie IIS-Server, anwenden.

Platzieren Sie einen Computer mit einem neuen Host Intrusion Prevention-Client in einer geeigneten Profilgruppe, damit ihm die richtigen Sicherheitsrichtlinien zugewiesen werden. Wenn dies nicht möglich ist, können Sie eine Richtlinie für einen einzelnen Client einrichten, indem Sie die Richtlinien auf den einzelnen Knotenebenen ändern. Die meisten übernommenen Richtlinien können überschrieben werden, sofern einer Richtlinie keine erzwungene Übernahme zugewiesen ist.

Wenn die ePolicy Orchestrator-Strukturknoten bereits so organisiert wurden, dass sie Produkte unterstützen, deren Organisation nicht zur Host Intrusion Prevention passt, kann es schwierig sein, die Struktur zu reorganisieren. Da die Reorganisation vorhandene Richtlinienzuweisungen unterbrechen kann, ist es erforderlich, alle Berechtigungen für alle anwendbaren Produkte zu kennen.

Kann ich die auf einen bestimmten Knoten oder Clients anwendbaren Richtlinien anzeigen oder bearbeiten?

Ja. Host Intrusion Prevention besitzt bestimmte Kategorien, wie IPS-Regeln und den IPS-Schutz, die jeweils unterschiedliche Einstellungen ermöglichen. Innerhalb der Host Intrusion Prevention-Funktionen finden Sie auf der Registerkarte „Richtlinien“ die Kategorien des ausgewählten Knotens. Jede Kategorie zeigt die Namen der ihr zugewiesenen Richtlinien an. Wie der „IPS-Schutz“ weisen die meisten Kategorien nur eine Richtlinie auf, während die Kategorien „IPS-Regeln“ und „Vertrauenswürdige Anwendungen“ auch mehrere Richtlinieninstanzen besitzen können. Um die Einzelheiten zu jeder Richtlinie anzuzeigen, klicken Sie auf den Namen der Richtlinie.

Wie kann ich alle verfügbaren Richtlinien und die Knoten anzeigen, denen diese zugewiesen sind?

Die ePolicy Orchestrator-Struktur besitzt einen Knoten „Richtlinienkatalog“, der eine Liste aller, in jeder Kategorie vorhandenen Richtlinien und die Anzahl der Zuweisungen anzeigt. Klicken Sie auf den Zählerwert, um eine Liste aller Knoten anzuzeigen, denen die Richtlinie direkt zugewiesen wird. Der Zähler enthält nicht die Knoten, an die die Richtlinie vererbt wurde.

Wie kann ich die durch Clients ausgelösten IPS-Ereignisse anzeigen?

ePolicy Orchestrator besitzt keinen eigenen Ereignis-Viewer. Daher werden Ereignisse innerhalb der Richtlinie „IPS-Regeln“ über die Host Intrusion Prevention-Registerkarte „IPS-Ereignisse“ behandelt. Um die Liste der mit einem ausgewählten Knoten verbundenen Ereignisse anzuzeigen, klicken Sie auf die Registerkarte „Richtlinien“ und dann auf die Verknüpfung „IPS-Ereignisse“. Die Registerkarte „IPS-Ereignisse“ enthält den gesamten Satz aller durch Clients unter dem ausgewählten Knoten für eine bestimmte Anzahl von Tagen generierten IPS-Ereignisse. Die Anzeige wird automatisch aktualisiert, sobald neue Ereignisse ausgelöst werden. Folgende Optionen sind verfügbar:

- Sortieren der Ereignisse anhand eines bestimmten Attributs oder Filtern der Ereignisse anhand mehrerer Attribute.
- Anzeigen von Ereignisdetails.

- Markieren von Ereignissen als gelesen oder als verborgen und Anzeigen der Ereignisse als Kombinationen aus gelesenen, ungelesenen und verborgenen Ereignissen.
- Erstellen von Ausnahmen oder von ereignisbasierten vertrauenswürdigen Anwendungen.

Wie erstelle ich eine auf einem IPS-Ereignis basierende Ausnahme?

Wählen Sie auf der Registerkarte „IPS-Ereignisse“ ein einzelnes Ereignis aus und klicken Sie auf **Ausnahme erstellen**. Ein auf der Grundlage des Originalereignisses vorbelegtes Dialogfeld „Neue Ausnahme“ wird geöffnet. Auf einer Registerkarte des Dialogfelds „Neue Ausnahme“ wird eine Liste der Zielinstanzen der IPS-Regelrichtlinie angezeigt, in der Sie die Ausnahme beim Erstellen platzieren.

Die neue Ausnahme kann nur in einer bestehenden Richtlinie platziert werden, die bearbeitet werden kann.

Wenden Sie eine Ausnahme entweder auf einen bestimmten Client oder auf eine Vielzahl von Clients an – Zielrichtlinie für eine Ausnahme kann entweder eine bestimmte Client-Richtlinie sein oder eine, die einem verbreiteten Profil entspricht. Alle Richtlinien sind jedoch standardmäßig freigegeben und erscheinen in der Zuweisungsliste aller Knoten. Es empfiehlt sich, eine geringe Anzahl von Richtlinien, die gemeinsam die Anforderungen aller Clients erfüllen, sorgfältig zu erstellen und zu warten.

Anstatt eine neue Ausnahme zu erstellen, können Sie auch eine in einer Richtlinie vorhandene Ausnahme mit ähnlichen Attributen bearbeiten. Hierzu verwenden Sie die Funktion für die Suche nach ähnlichen Ausnahmen.

Wie kann ich die IPS-Regelrichtlinien mithilfe des automatischen Tuning-Mechanismus verfeinern?

Host Intrusion Prevention bietet die Option des adaptiven Modus. Damit können Clients automatisch und ohne Rückmeldung Client-Regeln erstellen, die blockierte, aber unschädliche Aktivitäten zulassen. Wenn Clients über einen gewissen Zeitraum im adaptiven Modus gearbeitet haben, können Administratoren:

- die Liste der für Clients mit ähnlichem Profil erstellen Regeln anzeigen und auf der Grundlage dieser Information eine neue Richtlinie erstellen. diese neue Richtlinie kann dann auf weitere Clients mit demselben Profil angewendet werden.
- ermitteln, ob bestimmte Client-Regeln einen Sicherheitsverstoß darstellen und diese im Rahmen der IPS-Regelrichtlinie blockieren.
- eine aggregierte Liste der Ausnahmen anzeigen, um zu erfahren, ob derselbe Vorgang bei unterschiedlichen Clients mit demselben Profil vorherrscht.
- eine Client-Ausnahmeregel in die Liste der Richtlinienausnahmen verschieben.
- vorhandene Richtlinienausnahmen suchen, um eine der Client-Ausnahme ähnliche Ausnahme zu finden, die bearbeitet werden kann.

Wie erstelle ich benutzerdefinierte Signaturen für eine IPS-Richtlinie?

Benutzerdefinierte Signaturen sind Teil der IPS-Regelrichtlinie. Sie können im Rahmen der spezifischen Sicherheitsanforderungen eines Profils erstellt werden. Für einfache Signaturen ist ein Assistent für benutzerdefinierte Signaturen verfügbar. Fortschrittliche Benutzer verwenden den Standard- oder den Expertenmodus.

Wie reorganisiere ich vorhandene Ausnahmen und benutzerdefinierte Signaturen in einer neuen Richtlinie?

Sie haben als Administrator bei einigen Clients Falsch-Positiv-Meldungen gefunden und dafür Ausnahmen erstellt. Da diese Falsch-Positiv-Ereignisse vereinzelt auftraten, haben Sie sie in verschiedenen Richtlinien platziert. Auf den zweiten Blick erkennen Sie ein neues Muster, das in einer eigenen Richtlinie isoliert werden kann.

Um diese Ausnahmen in einer neuen Richtlinie zu reorganisieren, müssen Sie eine neue IPS-Regelrichtlinie erstellen und diese zur Liste der IPS-Regelrichtlinien für den entsprechenden Knoten hinzufügen. Zeigen Sie die Liste aller Ausnahmen der verschiedenen, diesem Knoten zugewiesenen Richtlinien an. Wählen Sie die entsprechenden Ausnahmen aus und verschieben Sie diese in die neue Richtlinie.

Diese neue Richtlinie kann dann auf weitere Clients angewendet werden, die einzeln oder als Gruppe zu dem neu festgestellten Profil passen.

Wie finde ich vorhandene Richtlinien, die mit einem bestimmten Profil übereinstimmen?

In der Regel besitzt ein Unternehmen mehrere IPS-Regelrichtlinien – je eine pro Client-Profil, wie IIS-Server und SQL-Server. Typischerweise verwalten mehrere Administratoren verschiedene Teile des Systems, wobei sie häufig in unterschiedlichen Schichten arbeiten. Daher ist es von essenzieller Bedeutung, eine kleine Anzahl gut gewarteter Richtlinien zu besitzen. Dies erleichtert Administratoren das schnelle Verständnis der aktuellen Richtlinienorganisation und sie finden schneller das, was sie suchen.

Mit der Suchfunktion für IPS-Ausnahmeregeln können Sie Ausnahmen auf der Grundlage ihrer Attribute suchen und deren im Prozess übergeordnete Richtlinie ermitteln. Die Suchfunktion bietet folgende Möglichkeiten:

- Nach Richtlinien zu suchen, die eine Ausnahme für eine Anwendung enthalten.
- Nach für eine Signatur erstellten Richtlinien zu suchen.
- Nach Richtlinien zu suchen, die Ausnahmen enthalten, die mit einem oder mehreren Attributen eines Falsch-Positiv-Ereignisses übereinstimmen.

A Schreiben von benutzerdefinierten Signaturen

In diesem Kapitel wird die Struktur von benutzerdefinierten Signaturen beschrieben. Außerdem finden Sie hier Informationen über das Schreiben von benutzerdefinierten Signaturen für die verschiedenen Client-Plattformen. Themen:

- *Regelstruktur*
- *Benutzerdefinierte Windows-Signaturen*
- *Benutzerdefinierte Solaris-Signaturen*
- *Benutzerdefinierte Linux-Signaturen*

Regelstruktur

Jede Signatur umfasst eine oder mehrere *Regeln*, die in der Syntax der ANSI-TCL-Sprache (Tool Command Language) geschrieben sind. Jede Regel enthält obligatorische und optionale *Abschnitte*, wobei jede Zeile einen Abschnitt enthält. Optionale Abschnitte sind vom Betriebssystem und der Regelklasse abhängig. Jeder Abschnitt definiert eine Regelkategorie und einen Wert. Ein Abschnitt bezeichnet stets die Regelklasse, die das gesamte Verhalten der Regel definiert.

Grundstruktur einer Regel:

```
Rule {
   Abschnitt A Wert
   Abschnitt B Wert
   Abschnitt C Wert
   ...
   }
```

Überprüfen Sie unbedingt die Regeln für das Schreiben von Zeichenfolgen und Escape-Zeichenfolgen in TCL, bevor Sie versuchen, benutzerdefinierte Regeln zu schreiben. Eine schnelle Überprüfung sämtlicher Standardreferenzen auf TCL sollte gewährleisten, dass Sie die richtigen Werte ordnungsgemäß eingeben.

Eine Regel, die eine Anforderung an einen Webserver verhindert, die „Betreff“ in der HTTP-Anforderungsanfrage enthält, hat das folgende Format:

```
Rule {
   Class Isapi
   Id 4001
   level 4
   query { Include „*Betreff*“ }
   method { Include „GET“ }
   time { Include „*“ }
   application { Include „*“}
   user_name { Include „*“ }
   directives -c -d isapi:request
   }
```

Eine Erläuterung der verschiedenen Abschnitte und Werte finden Sie unter *Benutzerdefinierte Windows-Signaturen* auf Seite 184.

Obligatorische allgemeine Abschnitte

Zu den obligatorischen Abschnitten einer Regel und deren Werten gehören die nachfolgenden Elemente. Die für den ausgewählten Abschnitt *class* obligatorischen Abschnitte finden Sie im Klassenabschnitt unter *Benutzerdefinierte Windows-, Unix- und Linux-Signaturen*. Die Schlüsselwörter *Include* und *Exclude* werden für alle Abschnitte mit Ausnahme von „Id“, „level“ und „directives“ verwendet. *Include* bedeutet, dass der Abschnitt für den angegebenen Wert gilt, und *Exclude* bedeutet, dass der Abschnitt für alle Werte mit Ausnahme des angegebenen Werts gilt.

Abschnittsname	Wert	Beschreibung
Class	Abhängig vom Betriebssystem.	Gibt die Klasse an, für die diese Regel gilt. Siehe: ■ *Benutzerdefinierte Windows-Signaturen* auf Seite 184 ■ *Benutzerdefinierte Solaris-Signaturen* auf Seite 196 ■ *Benutzerdefinierte Linux-Signaturen* auf Seite 200
Id	4000 – 7999	Die eindeutige ID-Nummer der Signatur. Es handelt sich um die für benutzerdefinierte Regeln verfügbaren Nummern.
level	0 1 2 3 4	Die Sicherheitsebene der Signatur: ■ 0 = Deaktiviert ■ 1 = Weiß ■ 2 = Gelb ■ 3 = Orange ■ 4 = Rot
time	`{Include „*“}`	Dieser Abschnitt hat nur diesen einen Wert.

Abschnittsname	Wert	Beschreibung
user_name	{Include/Exclude „Benutzer oder Systemkonto“}	Die Benutzer, für die diese Regel gilt. Legen Sie bestimmte oder alle Benutzer fest. Anmerkungen für Windows: Für lokale Benutzer: Verwenden Sie <Rechnername>/<lokaler Benutzername>. Für Domänenbenutzer: Verwenden Sie <Domänenname>/<Domänenbenutzername>. Für lokales System: Verwenden Sie Lokal/System; dies entspricht NT-Autorität/System unter Windows NT und <Domäne>/<Computer> unter Windows 2000. Manche extern initiierte Aktionen berichten nicht die ID des externen Benutzers, sondern benutzen den lokalen Dienst und dessen Benutzerkontext. Sie müssen beim Entwickeln von Regeln eine entsprechende Planung vornehmen. Wenn ein Prozess im Kontext einer „Nullsitzung“ vorkommt, sind Benutzer und Domäne „anonym“. Wenn eine Regel für alle Benutzer gilt, verwenden Sie *. Unter Solaris muss für diesen Abschnitt die Groß- und Kleinschreibung beachtet werden.
application	{Include/Exclude „Pfad- und Anwendungsname“}	Der vollständige Pfad des Prozesses, der die Instanz erstellende Operation durchgeführt hat. Wenn es sich um eine externe Operation handelt, ist die Anwendung der lokale Dienst/Server, der die Operation durchführt. Manche lokalen Operationen werden wie externe Operationen behandelt. Beispielsweise ist unter Windows der Anwendungsname der lokale Dienst/Server, der die Operation durchgeführt hat. Wenn eine Regel für alle Anwendungen gilt, verwenden Sie *. Unter Solaris muss für diesen Abschnitt die Groß- und Kleinschreibung beachtet werden.
directives -c -d	Operationstyp	Die Operationstypen sind klassenabhängig und werden in den nachfolgenden Abschnitten für jede Klasse aufgelistet. Beachten Sie, dass die Schalter -c und -d verwendet werden müssen.

Sie können eine Signatur mit mehreren Regeln erstellen, indem Sie die Regeln nacheinander hinzufügen. Beachten Sie, dass jede Regel in derselben Signatur denselben Wert für die Abschnitte *id* und *level* haben muss.

Verwendung von „Include“ und „Exclude“

Wenn Sie einen Abschnittswert als *Include* markieren, gilt der Abschnitt für den angegebenen Wert. Wenn Sie einen Abschnittswert als *Exclude* markieren, gilt der *Abschnitt* für alle Werte mit Ausnahme des angegebenen. Wenn Sie diese Schlüsselwörter verwenden, sind sie in Klammern eingeschlossen { ... } und ihre Werte in Anführungszeichen „ ... “.

Um z. B. alle Textdateien zu überwachen unter **C:\test\:**

```
files { Include „C:\\test\\*.txt“ }
```

und um alle Dateien mit Ausnahme der Textdateien zu überwachen unter: **C:\test\:**

```
files { Exclude „C:\\test\\*.txt“ }
```

Kombinieren Sie die Schlüsselwörter, um Werte aus einem Satz von eingeschlossenen Werten auszuschließen. Um alle Textdateien zu überwachen im Ordner **C:\test** mit Ausnahme der Datei **abc.txt**:

```
files { Include „C:\\test\\*.txt“ }
files { Exclude „C:\\test\\abc.txt“ }
```

Bei jedem Hinzufügen desselben Abschnitts mit demselben Schlüsselwort fügen Sie eine Operation hinzu. So überwachen Sie beliebige Textdateien im Ordner **C:\test**, deren Name mit der Zeichenfolge „abc“ beginnt:

```
files { Include „C:\\test\\*.txt“ }
files { Include „C:\\test\\abc*“ }
```

Optionale allgemeine Abschnitte

Zu den allgemeinen optionalen Abschnitten einer Regel und deren Werten gehören die nachfolgenden Elemente. Informationen über optionale Abschnitte des ausgewählten Abschnitts *class* finden Sie im Abschnitt über Klassen unter *Benutzerdefinierte Windows-, Unix- und Linux-Signaturen*. Die Schlüsselwörter *Include* und *Exclude* werden sowohl für Abhängigkeiten als auch für Attribute verwendet. *Include* bedeutet, dass der Abschnitt für den angegebenen Wert gilt, und *Exclude* bedeutet, dass der Abschnitt für alle Werte mit Ausnahme des angegebenen Werts gilt.

Abschnitt	Wert	Beschreibung
dependencies -c -d	{Include/Exclude „ID einer Regel“}	Definiert Abhängigkeiten zwischen Regeln und verhindert das Auslösen von abhängigen Regeln. Es werden nur die Schalter -c und -d verwendet.

Verwenden des Abschnitts dependencies

Fügen Sie den optionalen Abschnitt *dependencies* hinzu, um zu verhindern, dass eine allgemeinere Regel zusammen mit einer spezifischeren Regel ausgelöst wird. Wenn es beispielsweise nur eine zu überwachende Regel gibt für eine einzelne Textdatei unter **C:\test**:

```
files { Include „C:\\test\\abc.txt“ }
```

sowie eine Regel zum Überwachen aller Textdateien unter **C:\test\:**

```
files { Include „C:\\test\\*.txt“ }
```

Fügen Sie den Abschnitt *dependencies* der spezifischeren Regel hinzu. Dieser Abschnitt teilt dem System im Wesentlichen mit, dass keine allgemeinere Regel ausgelöst wird, wenn die spezifischere Regel ausgelöst wird.

```
files { Include „C:\\test\\abc.txt“ }
dependencies -c -d „the general rule“
```

Abschnittswertvariablen

Platzhalter, Metasymbole und vordefinierte Variablen können als Wert in den verfügbaren Abschnitten verwendet werden.

- *Verwenden von Platzhaltern*.
- *Verwenden von Umgebungsvariablen*.
- *Verwenden von vordefinierten Variablen*.

Verwenden von Platzhaltern

Sie können Platzhalter für einen Teil der Abschnittswerte verwenden.

Zeichen	Bedeutung
? (Fragezeichen)	Ein einzelnes Zeichen.
***** (Sternchen)	Mehrere Zeichen. `user_name { Include „*“ }`
& (Kaufmännisches Und-Zeichen)	Mehrere Zeichen mit Ausnahme von / und \. Wird zum Abgleich der Root-Ebene eines Ordners mit Ausnahme der Unterordner verwendet. `files { Include „C:\\test\\&.txt“ }`
! (Ausrufezeichen)	Platzhalter-Escape-Zeichen. `files { Include „C:\\test\\yahoo!!.txt“ }`

Verwenden von Umgebungsvariablen

Verwenden Sie Umgebungsvariablen und den Befehl `iEnv` mit einem Parameter (der Variablenname) als schnelle Möglichkeit, Windows-Datei- und -Verzeichnispfadnamen einzugeben.

Umgebungsvariable	Bedeutung
iEnv SystemRoot	C:\winnt\, wobei C das Laufwerk mit dem Windows-Systemordner ist. Zum Beispiel: `files {Include „[iEnv SystemRoot]\\ system32\\abc.txt“ }`
iEnv SystemDrive	C:\ wobei C das Laufwerk mit dem Windows-Systemordner ist. Zum Beispiel: `files {Include „[iEnv System Root]\\ system32\\abc.txt“ }`

Verwenden von vordefinierten Variablen

Host Intrusion Prevention ermöglicht vordefinierte Variablen für das Schreiben von Regeln. Diesen Variablen wird „$“ vorangestellt; sie sind nachfolgend aufgeführt.

Windows IIS Web Server

Variable	Bedeutung
IIS_BinDir	Verzeichnis, in dem sich inetinfo.exe befindet
IIS_Computer	Name des Computers, auf dem IIS ausgeführt wird
IIS_Envelope	Beinhaltet alle Dateien, auf die IIS zugreifen kann
IIS_Exe_Dirs	Virtuelle Verzeichnisse, die die Ausführung der Dateien zulassen, einschließlich des System-Roots und des IIS-Root
IIS_Ftp_Dir	Root-Verzeichnisse der FTP-Site
IIS_FTP_USR	Kontoname des anonymen Benutzers des lokalen FTP-Servers
IIS_FtpLogDir	FTP-Protokolldateienverzeichnis
IIS_IUSR	Kontoname des anonymen Benutzers des lokalen Webservers
IIS_IUSRD	Kontoname des anonymen Benutzers des Domänen-Webservers
IIS_IWAM	IIS Web Application Manager-Benutzerkontoname
IIS_LogFileDir	Web-Protokolldateienverzeichnis
IIS_LVirt_Root	Alle virtuellen IIS-Verzeichnisse
IIS_Processes	Prozesse mit Zugriffsrechten auf IIS-Ressourcen
IIS_Services	Alle Dienste, die erforderlich sind, damit IIS ordnungsgemäß ausgeführt werden kann

MS SQL-Datenbankserver

MSSQL_Allowed_Access_Paths	Verzeichnisse, wie \WINNT und \WINNT\System32, auf die zugegriffen werden kann
MSSQL_Allowed_Execution_Paths	Verzeichnisse, wie \WINNT und \WINNT\System32, die ausgeführt werden können
MSSQL_Allowed_Modification_Paths	Verzeichnisse, wie \WINNT\Temp, die bearbeitet werden können.
MSSQL_Auxiliary_Services	Die zusätzlichen im System gefundenen MS SQL-Dienste
MSSQL_Core_Services	Die zentralen MS SQL-Dienste, die im System gefunden wurden
MSSQL_Data_Paths	Alle anderen Datendateien, die mit MS SQL in Verbindung stehen und sich außerhalb des Verzeichnisses „MSSQL_DataRoot_Path“ befinden
MSSQL_DataRoot_Paths	Der Pfad zu den jeweiligen MS SQL-Dateien für jede Instanz
MSSQL_Instances	Der Name aller installierten MS SQL-Instanzen
MSSQL_Registry_Paths	Alle Registrierungsspeicherorte, die mit MS SQL verknüpft sind

Solaris Apache und iPlanet

Variable	Bedeutung
UAPACHE_Bins	Pfad zu den Apache-Binärdateien
UAPACHE_CgiRoots	Pfad zu den CGI-Root-Verzeichnissen
UAPACHE_ConfDirs	Verzeichnisse, die die Apache-Konfigurationsdateien enthalten
UAPACHE_DocRoots	Pfad zu den Dokument-Root-Verzeichnissen
UAPACHE_Logs	Apache-Protokolldateien
UAPACHE_Logs_dir	Protokolldateiverzeichnis
UAPACHE_Roots	Apache-Web-Root-Dateien
UAPACHE_Users	Benutzer, die Apache ausführen als
UAPACHE_VcgiRoots	Pfad zu den CGI-Root-Verzeichnissen von virtuellen Servern
UAPACHE_VdocRoots	Virtuelle Dokument-Root-Verzeichnisse
UAPACHE_Vlogs	Protokolldateien der virtuellen Server
UAPACHE_Vlogs_dir	Verzeichnisse für die Protokolldateien der virtuellen Server
UIPLANET_BinDirs	Pfad zu den iPlanet-Binärdateien
UIPLANET_CgiDirs	Pfad zu den CGI-Verzeichnissen
UIPLANET_DocDirs	Pfad zu den Dokumentverzeichnissen
UIPLANET_Process	Pfad zur iPlanet ns-httpd-Binärdatei
UIPLANET_Roots	Pfad zu den iPlanet-Root-Verzeichnissen

Benutzerdefinierte Windows-Signaturen

Dieses Thema beschreibt, wie benutzerdefinierte Windows-Signaturen geschrieben werden.

Regeln in den Windows-class-Dateien verwenden doppelte Schrägstriche, und Regeln in den UNIX_Files der Solaris-Klasse verwenden einen einzelnen Schrägstrich.

Der Klassenabschnittswert hängt von der Natur des Sicherheitsproblems ab und vom Schutz, den die Regeln bieten können. Für Windows sind diese Werte verfügbar:

Class	Verwendung
Dateien	Für Datei- oder Verzeichnisoperationen. Siehe *Klassendateien*.
Isapi	Für die Überwachung von Anforderungen an IIS. Siehe *Klasse „Isapi“* auf Seite 187.
Registrierung	Für Registrierungsschlüssel und Wertoperationen. Siehe *Klasse „Registry“* auf Seite 191.
Dienste	Für Dienstoperationen. Siehe *Klasse „Services“* auf Seite 193.

Klassendateien

In der folgenden Tabelle sind die möglichen Abschnitte der Klasse *Files* aufgeführt.

Abschnitt	Werte	Hinweise
Class	Files	
Id	4000 – 7999	
level	0, 1, 2, 3, 4	
time	*	
user-name	Systemkontobenutzer	
application	Pfad- und Anwendungsname	
files	An der Operation beteiligte Datei oder Ordner	Siehe Hinweis 1, 2.
dest_file	Zieldatei, wenn an der Operation Ursprungs- und Zieldateien beteiligt ist.	Dieser Abschnitt ist optional. Siehe Hinweis 1, 2.
directives -c -d	files:create	Direktes Erstellen oder Verschieben der Datei in das Verzeichnis.
	files:read	Öffnen der Datei im Lesemodus.
	files:write	Öffnen der Datei im Schreibmodus.
	files:execute	Ausführen der Datei (Ausführen eines Verzeichnisses bedeutet, dass dieses Verzeichnis zum aktuellen Verzeichnis wird).
	files:delete	Löschen der Datei aus einem Verzeichnis oder Verschieben in ein anderes Verzeichnis.

Abschnitt	Werte	Hinweise
	files:rename	Umbenennen einer Datei im selben Verzeichnis, siehe Hinweis 2.
	files:attribute	Ändern der Dateiattribute Überwachte Attribute sind „Schreibgeschützt“, „Verborgen“, „Archiv“ und „System“. Die für Windows 2000 spezifischen Attribute „Index“, „Komprimieren“ und „Verschlüsseln“ werden nicht überwacht.

Hinweis 1

Wenn der Abschnitt *files* verwendet wird, kann der Pfad zu einem überwachten Ordner entweder ein vollständiger Pfad oder ein Platzhalter sein. Bei den folgenden Beispielen handelt es sich um gültige Pfaddarstellungen:

```
files { Include „C:\\test\\abc.txt“ }

files { Include „*\\test\\abc.txt“ }

files { Include „*\\abc.txt“ }
```

Wenn der Abschnitt *dest_files* verwendet wird, kann der absolute Pfad nicht verwendet werden und ein Platzhalter muss am Beginn des Pfades vorhanden sein, um das Laufwerk darzustellen. Bei den folgenden Beispielen handelt es sich um gültige Pfaddarstellungen:

```
dest_file { Include „*\\test\\abc.txt“ }

dest_file { Include „*\\abc.txt“ }
```

Hinweis 2

Die Direktive *files:rename* hat eine andere Bedeutung, wenn sie mit Abschnitt *files* und Abschnitt *dest_file* kombiniert wird.

- In Kombination mit dem Abschnitt *files* bedeutet sie, dass die Umbenennung der Datei im Abschnitt *files* überwacht wird. Die folgende Regel überwacht z. B. das Umbenennen der Datei C:\test\abc.txt auf einen anderen Namen:

```
Rule {
   Class Files
   Id 4001
   level 1
   files { Include „C:\\test\\abc.txt“ }
   time { Include „*“ }
   application { Include „*“}
   user_name { Include „*“ }
   directives -c -d files:rename
   }
```

- In Kombination mit dem Abschnitt *dest_files* bedeutet sie, dass keine Datei in die Datei im Abschnitt *dest_files* umbenannt werden kann. Die folgende Regel überwacht z. B. das Umbenennen einer beliebigen Datei in C:\test\abc.txt:

```
Rule {
   Class Files
   Id 4001
   level 1
   dest_file { Include „*\\test\\abc.txt“ }
   time { Include „*“ }
   application { Include „*“}
   user_name { Include „*“ }
   directives -c -d files:rename
}
```

Der Abschnitt *files* ist nicht obligatorisch, wenn der Abschnitt *dest_file* verwendet wird. Wenn der Abschnitt *files* verwendet wird, müssen die beiden Abschnitte *files* und *dest_file* nicht übereinstimmen.

Erweiterte Details

Einige oder alle der folgenden Parameter werden in der Registerkarte „Erweiterte Details“ von Sicherheitsereignissen für die Klasse *Files* angezeigt. Die Werte dieser Parameter können verdeutlichen, weshalb eine Signatur ausgelöst wird.

Name der grafischen Benutzeroberfläche	Erklärung
Dateien	Name der Datei, auf die ein Zugriff erfolgte
dest file	Gilt nur beim Umbenennen von Dateien: Neuer Name, auf den die Datei geändert wurde

Die folgende Regel würde verhindern, dass ein Benutzer oder ein Prozess die Datei „abc.txt“ im Ordner C:\test\ erstellt.

```
Rule {
   Class Files
   Id 4001
   level 4
   files { Include „C:\\test\\abc.txt“ }
   time { Include „*“ }
   application { Include „*“}
   user_name { Include „*“ }
   directives -c -d files:create
   }
```

Die verschiedenen Abschnitte dieser Regel haben die folgende Bedeutung:

- Class Files: Gibt an, dass diese Regel für die Dateioperationenklasse gilt.
- Id 4001: Weist die ID 4001 dieser Regel zu. Wenn für eine benutzerdefinierte Signatur mehrere Regeln gelten, müsste jede dieser Regeln dieselbe ID verwenden.

- level 4: Weist der Regel die Sicherheitsebene „Hoch“ zu. Wenn für eine benutzerdefinierte Signatur mehrere Regeln gelten, müsste jede dieser Regeln dieselbe Ebene verwenden.
- files { Include „C:\\test\\abc.txt“ }: Gibt an, dass diese Regel die bestimmte Datei und den Pfad C:\test\abc.txt abdeckt. Wenn eine Regel mehrere Dateien abdecken soll, müssten sie in diesem Abschnitt in anderen Zeilen hinzugefügt werden. Zum Überwachen der Dateien C:\test\abc.txt und C:\test\xyz.txt ändert sich der Abschnitt in: files { Include „C:\\test\\abc.txt“ „C:\\test\\xyz.txt“ }.
- time { Include „*“ }: Dieser Abschnitt wird gegenwärtig nicht verwendet, muss jedoch auf diese Weise in der Regel enthalten sein.
- application { Include „*“}: Gibt an, dass diese Regel für alle Prozesse gilt. Wenn Sie die Regel auf bestimmte Prozesse beschränken möchten, müssten diese hier mit ihrem vollständigen Pfadnamen ausgedrückt werden.
- user_name { Include „*“ }: Gibt an, dass diese Regel für alle Benutzer gilt (oder genauer gesagt, den Sicherheitskontext, in dem ein Prozess ausgeführt wird). Wenn Sie die Regel auf bestimmte Benutzerkontexte beschränken möchten, müssten diese hier in der Form „Lokal/Benutzer“ oder „Domäne/Benutzer“ ausgedrückt werden. Einzelheiten dazu finden Sie im Abschnitt unter „Obligatorische allgemeine Abschnitte“.
- directives -c -d files:create: Gibt an, dass diese Regel die Erstellung einer Datei abdeckt. Die Schalter -c und -d müssen im Abschnitt „directives“ stets verwendet werden.

Klasse „Isapi“

In der folgenden Tabelle sind die möglichen Abschnitte der Klasse *Isapi* aufgeführt.

Abschnitt	Werte	Hinweise
Class	Isapi	
Id	4000 – 7999	
level	0, 1, 2, 3, 4	
time	*	
user_name	Benutzer- oder Systemkonto	
application	Pfad- und Anwendungsname	
url		Dieser Abschnitt ist optional. Dieser Abschnitt wird mit dem URL-Teil einer eingehenden Anforderung abgeglichen, siehe Hinweise 1, 2, 3, 4.
query		Dieser Abschnitt ist optional. Dieser Abschnitt wird mit dem „query“-Teil einer eingehenden Anforderung abgeglichen, siehe Hinweise 1, 2, 3, 4.
method	„GET“, „POST“, „INDEX“ und alle anderen erlaubten HTTP-Methoden.	Dieser Abschnitt ist optional. Siehe Hinweis 4.
directives -c -d	isapi:request	

Hinweis 1

Eine eingehende HTTP-Anforderung kann dargestellt werden als: http://www.myserver.com/{url}?{query}. In diesem Dokument verstehen wir unter {url} den „URL"-Teil der HTTP-Anforderung und {query} als den „Query"-Teil der HTTP-Anforderung. Mit dieser Namenskonvention können wir sagen, dass der Abschnitt „url" abgeglichen wird mit {url} und der Abschnitt „query" abgeglichen wird mit {query}.

Beispielsweise würde die folgende Regel ausgelöst, wenn die HTTP-Anfrage `http://www.myserver.com/search/abc.exe?subject=wildlife&environment=ocean` durch IIS empfangen würde:

```
Rule {
   Class Isapi
   Id 4001
   level 1
   url { Include „*abc*" }
   time { Include „*" }
   application { Include „*"}
   user_name { Include „*" }
   directives -c -d isapi:request
   }
```

Diese Regel wird ausgelöst, weil {url}=/search/abc.exe, wodurch der Wert des Abschnitts „url" abgeglichen wird (d. h. abc).

Hinweis 2

Bevor der Abgleich durchgeführt wird, werden die Abschnitte „url" und „query" dekodiert und normalisiert, sodass Anforderungen nicht mit Kodierungs- oder Escape-Sequenzen gefüllt werden können.

Hinweis 3

Eine Beschränkung für die maximale Länge kann für die Abschnitte „url" und „query" festgelegt werden. Durch Hinzufügen von „`;number-of-chars`" zum Wert dieser Abschnitte kann diese Regel nur abgeglichen werden, wenn {url} oder {query} aus mehr Zeichen besteht als „number-of-chars". Für die folgende Regel wird z. B. eine Übereinstimmung gefunden, wenn der URL-Teil der Anforderung „abc" enthält und als 500 Zeichen umfasst:

```
Rule {
   Class Isapi
   Id 4001
   level 1
   url { Include „*abc*;500" }
   time { Include „*" }
   application { Include „*"}
   user_name { Include „*" }
   directives -c -d isapi:request}
   }
```

Hinweis 4

Eine Regel muss mindestens eine der optionalen Abschnitte „url“, „query“ und „method“ enthalten.

Erweiterte Details

Einige oder alle der folgenden Parameter werden in der Registerkarte „Erweiterte Details“ von Sicherheitsereignissen für die Klasse *Isapi* angezeigt. Die Werte dieser Parameter können verdeutlichen, weshalb eine Signatur ausgelöst wird.

Name der grafischen Benutzeroberfläche	Erklärung
url	Dekodierter und normalisierter Adressteil einer eingehenden HTTP-Anforderung (der Teil vor dem „?“).
query	Dekodierter und normalisierter Anforderungsteil einer eingehenden HTTP-Anfrage (der Teil nach dem ersten „?“).
web server type	Typ und Version der verwendeten Webserver-Anwendung.
method	Methode einer eingehenden HTTP-Anforderung (wie „Get“, „Put“, „Post“, „Query“ usw.).
local file	Physischer Name der Datei, für die ein Abruf durch die Anforderung durchgeführt oder versucht wird. Dekodiert und normalisiert unter IIS.
raw url	„Raw“ (weder dekodierte noch normalisierte) Anforderungszeile der eingehenden HTTP-Anforderung. Anforderungszeile ist „<Methode> <Adresse[?query]> <HTTP-Version> CRLF“.
Benutzer	Benutzername des Client, der die Anforderung durchführt; nur verfügbar, wenn die Anforderung authentifiziert ist.
source	Client-Name oder IP-Adresse des Computers, von dem die HTTP-Anfrage stammt.
server	Daten über den Webserver, auf dem das Ereignis erstellt wird (das Gerät, auf dem der Client installiert ist) in der Form <Hostname>:<IP-Adresse>:<Port>. Der Hostname ist die Host-Variable aus der HTTP-Kopfzeile; er bleibt leer, wenn er nicht verfügbar ist.
content len	Zahl der Bytes im Fließtext des Mitteilungsabschnitts der Anforderung.

Die folgende Regel würde eine Anforderung an den Webserver verhindern, die „Betreff“ im Anforderungsteil der HTTP-Anforderung enthält:

```
Rule {
   Class Isapi
   Id 4001
   level 4
   query { Include „*Betreff*“ }
   method { Include „GET“ }
   time { Include „*“ }
   application { Include „*“}
   user_name { Include „*“ }
   directives -c -d isapi:request

   }
```

Beispielsweise würde die GET-Anforderung *http://www.myserver.com/test/abc.exe?subject=wildlife&environment=ocean* durch diese Regel verhindert.

Die verschiedenen Abschnitte dieser Regel haben die folgende Bedeutung:

- Class Isapi: Gibt an, dass diese Regel für die Isapi-Operationsklasse gilt.
- Id 4001: Weist die ID 4001 dieser Regel zu. Wenn für eine benutzerdefinierte Signatur mehrere Regeln gelten, müsste jede dieser Regeln dieselbe ID verwenden.
- level 4: Weist der Regel die Sicherheitsebene „Hoch“ zu. Wenn für eine benutzerdefinierte Signatur mehrere Regeln gelten, müsste jede dieser Regeln dieselbe Ebene verwenden.
- query { Include „*Betreff*“ }: Gibt an, dass die Regel mit einer beliebigen (GET)-Anforderung übereinstimmt, die die Zeichenfolge „Betreff“ im Anforderungsteil der HTTP-Anforderung enthält. Wenn die Regel mehrere Anforderungsteildateien abdecken soll, müssen Sie diese in diesem Abschnitt in anderen Zeilen hinzufügen.
- method { Include „GET“ }: Gibt an, dass die Regel nur GET-Anforderungen abgleichen kann.
- time { Include „*“ }: Dieser Abschnitt wird gegenwärtig nicht verwendet, muss jedoch auf diese Weise in der Regel enthalten sein.
- application { Include „*“}: Gibt an, dass diese Regel für alle Prozesse gilt. Wenn Sie die Regel auf bestimmte Prozesse beschränken möchten, müssten diese hier mit ihrem vollständigen Pfadnamen ausgedrückt werden.
- user_name { Include „*“ }: Gibt an, dass diese Regel für alle Benutzer gilt (oder genauer gesagt, für den Sicherheitskontext, in dem ein Prozess ausgeführt wird). Wenn Sie die Regel auf bestimmte Benutzerkontexte beschränken möchten, müssten diese hier in der Form „Lokal/Benutzer“ oder „Domäne/Benutzer“ ausgedrückt werden. Einzelheiten dazu finden Sie im Abschnitt unter „Obligatorische allgemeine Abschnitte“.
- directives -c -d isapi:request: Gibt an, dass diese Regel eine HTTP-Anforderung abdeckt. Die Schalter -c und -d müssen im Abschnitt „directives“ stets verwendet werden.

Klasse „Registry“

In der folgenden Tabelle sind die möglichen Abschnitte der Klasse *Registrierung* aufgeführt.

Abschnitt	Werte	Hinweise
Class	Registry	
Id	4000 – 7999	
level	0, 1, 2, 3, 4	
time	*	
user_name	Benutzer- oder Systemkonto	
application	Pfad- und Anwendungsname	
keys oder values	Registrierungsschlüssel oder -wert	Siehe Hinweis 1.
old data	Frühere Daten des Werts	Dieser Abschnitt ist optional. Er gilt nur für <Direktive> „Modify“; siehe Hinweis 2.
new data	Neue Daten des Werts	Dieser Abschnitt ist optional. Er gilt nur für <Direktive> „Modify“ oder „Create“; siehe Hinweis 2.
directives -c -d	registry:delete	Löschen eines Registrierungsschlüssels/-werts.
	registry:modify	Änderung des Inhalts eines Registrierungswerts oder Änderung der Daten eines Registrierungsschlüssels.
	registry:permissions	Änderung der Berechtigungen eines Registrierungsschlüssels.
	registry:read	Abrufen von Registrierungsschlüsseldaten (Nummer von Unterschlüsseln usw.) oder Abrufen des Inhalts eines Registrierungswerts.
	registry:enumerate	Aufzählung eines Registrierungschlüssels, d. h. Auflisten aller Unterschlüssel und Werte eines Schlüssels.

Hinweis 1

HKEY_LOCAL_MACHINE in einem Registrierungspfad wird ersetzt durch \REGISTRY\MACHINE\, und CurrentControlSet wird ersetzt durch ControlSet. Beispiel: Der Registrierungswert „abc“ unter dem Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa wird dargestellt als \\REGISTRY\\MACHINE\\SYSTEM\\ControlSet\\Control\\Lsa\\abc.

Hinweis 2

Die Daten der Abschnitte *old data* und *new data* müssen im Hexadezimal-Format vorliegen. Beispiel: Die Datendefinition des Registrierungswerts „\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\abc“ muss dargestellt werden als `old_data { Include „%64%65%66“}`.

Erweiterte Details

Einige oder alle der folgenden Parameter werden in der Registerkarte „Erweiterte Details“ von Sicherheitsereignissen für die Klasse *Registry* angezeigt. Die Werte dieser Parameter können verdeutlichen, weshalb eine Signatur ausgelöst wird.

Name der grafischen Benutzeroberfläche	Erklärung
Registry Key	Name des betroffenen Registrierungsschlüssels, einschließlich des Pfadnamens. Das Präfix \REGIS-TRY\MACHINE\ steht für HKEY_LOCAL_MACHINE\, und \REGISTRY\CURRENT_USER\ steht für \HKEY_USER\.
Registry Value(s)	Name des Registrierungswerts, verkettet mit dem vollständigen Schlüsselnamen.
old data New Data old data type new data type	Gilt nur für Änderungen des Registrierungswerts: Daten, die ein Registrierungwert enthielt, bevor er geändert wurde oder ein Änderungsversuch durchgeführt wurde. Gilt nur für Änderungen des Registrierungswerts: Daten, die ein Registrierungwert enthält, nachdem er geändert wurde, oder die er enthalten würde, wenn die Änderungen akzeptiert werden. Gilt nur für Änderungen des Registrierungswerts: Datentyp, den ein Registrierungswert enthält, bevor er geändert wird oder ein Änderungsversuch durchgeführt wurde. Gilt nur für Änderungen von Registrierungswerten: Datentyp, den ein Registrierungwert nach einer Änderung enthalten würde oder den er enthalten würde, wenn die Änderung akzeptiert würde.

Beispiel

Die folgende Regel würde verhindern, dass ein Benutzer oder ein Prozess den Registrierungswert „abc“ unter dem Registrierungsschlüssel „\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa“ löscht

```
Rule {
   Class Registry
   Id 4001
   level 4
   values { Include „\\REGISTRY\\MACHINE\SYSTEM\\ControlSet\\Control\\Lsa\\abc“ }
   time { Include „*“ }
   application { Include „*“}
   user_name { Include „*“ }
   directives -c -d registry:delete
   }
```

Die verschiedenen Abschnitte dieser Regel haben die folgende Bedeutung:

- Class Registry: Gibt an, dass diese Regel für Anforderungen gilt, die an IIS gesendet werden.
- Id 4001: Weist die ID 4001 dieser Regel zu. Wenn für eine benutzerdefinierte Signatur mehrere Regeln gelten, müsste jede dieser Regeln dieselbe ID verwenden.
- level 4: Weist der Regel die Sicherheitsebene „Hoch“ zu. Wenn für eine benutzerdefinierte Signatur mehrere Regeln gelten, müsste jede dieser Regeln dieselbe Ebene verwenden.

- values { Include „\\REGISTRY\\MACHINE\SYSTEM\\ControlSet\\Control\\Lsa\\abc“ }: Gibt an, dass die Regel den Registrierungswert „abc“ überwacht unter dem Registrierungsschlüssel „\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa“. Wenn die Regel mehrere Werte abdecken soll, müssen Sie diese in diesem Abschnitt in anderen Zeilen hinzufügen.
- time { Include „*“ }: Dieser Abschnitt wird gegenwärtig nicht verwendet, muss jedoch auf diese Weise in der Regel enthalten sein.
- application { Include „*“}: Gibt an, dass diese Regel für alle Prozesse gilt. Wenn Sie die Regel auf bestimmte Prozesse beschränken möchten, müssten diese hier mit ihrem vollständigen Pfadnamen ausgedrückt werden.
- user_name { Include „*“ }: Gibt an, dass diese Regel für alle Benutzer gilt (oder genauer gesagt, den Sicherheitskontext, in dem ein Prozess ausgeführt wird). Wenn Sie die Regel auf bestimmte Benutzerkontexte beschränken möchten, müssten diese hier in der Form „Lokal/Benutzer“ oder „Domäne/Benutzer“ ausgedrückt werden. Einzelheiten dazu finden Sie im Abschnitt unter „Obligatorische allgemeine Abschnitte“.
- directives -c -d registry:delete: Gibt an, dass diese Regel das Löschen eines Registrierungsschlüssels oder Werts abdeckt. Die Schalter -c und -d müssen im Abschnitt „directives“ stets verwendet werden.

Klasse „Services“

In der folgenden Tabelle sind die möglichen Abschnitte der Klasse *Dienste* aufgeführt.

Abschnitt	Werte	Bedeutung/Anmerkungen
Class	Services	
Id	4000 – 7999	
level	0, 1, 2, 3, 4	
time	*	
user_name	Benutzer- oder Systemkonto	
application	Pfad- und Anwendungsname	
services	Name des Dienstes, der das Subjekt der Operation ist, die die Instanz erstellt	Entweder muss der Abschnitt „services“ oder „display_names“ verwendet werden; der Name eines Dienstes befindet sich in der Registrierung unter HKLM\SYSTEM\CurrentControlSet\Services\; siehe Hinweis 1
display_names	Angezeigter Name des Dienstes	Dieser Name wird in der Systemsteuerung des Dienstes angezeigt, siehe Hinweis 1
directives -c -d	services:delete	Löschen eines Dienstes
	services:create	Erstellen eines Dienstes
	services:start	Geben eines Startbefehls an einen Dienst
	services:stop	Geben eines Stoppbefehls an einen Dienst
	services:pause	Geben eines Pausenbefehls an einen Dienst
	services:continue	Geben eines Fortsetzungsbefehls an einen Dienst
	services:startup	Ändern des Startmodus für einen Dienst
	services:profile_enable	Aktivieren eines Hardware-Profils
	services:profile_disable	Deaktivieren eines Hardware-Profils
	services:logon	Ändern der Anmeldeinformationen eines Dienstes

Hinweis 1

Der Abschnitt *service* muss den Namen des Dienstes des entsprechenden Registrierungsschlüssels unter HKLM_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ enthalten.

Der Abschnitt *display_names* muss den Anzeigenamen des Dienstes enthalten, d.h. den in der Systemsteuerung des Dienstes angezeigten Namen, der sich im folgenden Registrierungswert befindet: HKLM_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<Dienstname>\DisplayName.

Erweiterte Details

Einige oder alle der folgenden Parameter werden in der Registerkarte „Erweiterte Details“ von Sicherheitsereignissen für die Klasse *Services* angezeigt. Die Werte dieser Parameter können verdeutlichen, weshalb eine Signatur ausgelöst wird.

Name der grafischen Benutzeroberfläche	Erklärung	Mögliche Werte
display names	Name des Windows-Dienstes, so wie dieser in der Systemsteuerung des „Dienstemanagers“ angezeigt wird.	
services	Systemname des Windows-Dienstes (angezeigt unter HKLM\CurrentControlSet\Services\); dieser kann sich vom in der Systemsteuerung von „Dienstemanager“ angezeigten Namen unterscheiden.	
params	Gilt nur für das Starten eines Dienstes: An den Dienst bei Aktivierung übergebene Parameter.	
old startup	Gilt nur für das Erstellen oder Ändern des Startmodus eines Dienstes: gibt den Startmodus an, bevor er geändert wurde bzw. ein Änderungsversuch unternommen wurde.	Boot, System, Automatisch, Manuell, Deaktiviert
new startup	Gilt nur für das Ändern des Startmodus eines Dienstes: gibt den Startmodus an, der für einen Dienst nach seiner Änderung gilt bzw. den er hätte, wenn die Änderung akzeptiert wird.	Boot, System, Automatisch, Manuell, Deaktiviert
logon	Gilt nur für den Anmeldemodus eines Dienstes: Anmeldeinformationen (System oder Benutzerkonto), die durch den Dienst verwendet werden.	

Die folgende Regel würde die Deaktivierung des Alerter-Dienstes verhindern.

```
Rule {
   Class Services
   Id 4001
   level 4
   Service { Include „Alerter" }
   time { Include „*" }
   application { Include „*"}
   user_name { Include „*" }
   directives -c -d service:stop
   }
```

Die verschiedenen Abschnitte dieser Regel haben die folgende Bedeutung:

- Class Services: Gibt an, dass diese Regel für die Dateioperationenklasse gilt.
- Id 4001: Weist die ID 4001 dieser Regel zu. Wenn für eine benutzerdefinierte Signatur mehrere Regeln gelten, müsste jede dieser Regeln dieselbe ID verwenden.
- level 4: Weist der Regel die Sicherheitsebene „Hoch" zu. Wenn für eine benutzerdefinierte Signatur mehrere Regeln gelten, müsste jede dieser Regeln dieselbe Ebene verwenden.
- Service { Include „Alerter" }: Gibt an, dass diese Regel den Dienst mit dem Namen „Alerter" abdeckt. Wenn die Regel mehrere Dienste abdecken soll, müssen Sie sie in diesem Abschnitt in anderen Zeilen hinzufügen.
- time { Include „*" }: Dieser Abschnitt wird gegenwärtig nicht verwendet, muss jedoch auf diese Weise in der Regel enthalten sein.
- application { Include „*"}: Gibt an, dass diese Regel für alle Prozesse gilt. Wenn Sie die Regel auf bestimmte Prozesse beschränken möchten, müssten diese hier mit ihrem vollständigen Pfadnamen ausgedrückt werden.
- user_name { Include „*" }: Gibt an, dass diese Regel für alle Benutzer gilt (oder genauer gesagt, den Sicherheitskontext, in dem ein Prozess ausgeführt wird). Wenn Sie die Regel auf bestimmte Benutzerkontexte beschränken möchten, müssten diese hier in der Form „Lokal/Benutzer" oder „Domäne/Benutzer" ausgedrückt werden. Einzelheiten dazu finden Sie im Abschnitt unter „Obligatorische allgemeine Abschnitte".
- directives -c -d service:stop: Gibt an, dass diese Regel die Deaktivierung eines Dienstes abdeckt. Die Schalter -c und -d müssen im Abschnitt „directives" stets verwendet werden.

Benutzerdefinierte Solaris-Signaturen

Dieses Thema beschreibt, wie benutzerdefinierte Solaris-Signaturen geschrieben werden.

Regeln in den Windows-class-Dateien verwenden doppelte Schrägstriche, und Regeln in den UNIX_Files der Solaris-Klasse verwenden einen einzelnen Schrägstrich.

Die Klasse der Signatur hängt von der Natur des Sicherheitsproblems ab und vom Schutz, den die Regeln bieten können. Die Tabelle unten zeigt die verfügbaren Solaris-Klassen:

Klasse	Bedeutung/Anmerkungen
UNIX_file	Verwendet für Datei- oder Verzeichnisoperationen. Siehe *Klasse UNIX_file*.
UNIX_apache	Verwendet für http-Operationen. Siehe *Klasse UNIX_apache* auf Seite 198.

Klasse UNIX_file

In der folgenden Tabelle sind die möglichen Abschnitte der Klasse *Files* aufgeführt.

Abschnitt	Werte	Bedeutung/Anmerkungen
Class	UNIX_file	
Id	4000 – 7999	
level	0, 1, 2, 3, 4	
time	*	
user_name	Benutzer- oder Systemkonto	
application	Benutzer- oder Systemkontopfad + Anwendungsname	
Dateien	Quelldatei(en)	Zu suchende Dateien. Dies ist optional, wenn die Abschnittsquelle verwendet wird; siehe Hinweis 1.
source	Zieldateinamen	Dies ist optional. Siehe Hinweis 1.
Dateiberechtigung]	Liste der Berechtigungen für Quelldateinamen	Dies ist optional. Siehe Hinweis 2.
neue Berechtigung	Berechtigungsmodus für neu erstellte Datei oder veränderte Berechtigung	Dies ist optional. Siehe Hinweis 2.
Richtlinien	unixfile:symlink	Erstellen eines symbolischen Links.
	unixfile:link	Erstellen eines Hard-Links. Siehe Hinweis 3.
	unixfile:read	Öffnen der Datei im Lesemodus.
	unixfile:write	Öffnen der Datei im Schreibmodus.
	unixfile:unlink	Löschen einer Datei aus einem Verzeichnis oder Löschen des Verzeichnisses.
	unixfile:rename	Umbenennen der Datei. Siehe Hinweis 4.
	unixfile:chmod	Ändern der Berechtigungen für das Verzeichnis oder die Datei.
	unixfile:chown	Ändern der Dateieigentümerschaft des Verzeichnisses oder der Datei.
	unixfile:create	Erstellen einer Datei.

Abschnitt	Werte	Bedeutung/Anmerkungen
	unixfile:mkdir	Erstellen eines Verzeichnisses.
	unixfile:rmdir	Entfernen eines Verzeichnisses.
	unixfile:chdir	Ändern des Arbeitsverzeichnisses.

Hinweis 1

Relevante (X) Richtlinien pro Abschnitt:

directive	file	source	file permission	new permission
symlink	X	X	-	X
read	X	-	-	-
write	X	-	-	-
unlink	X	-	-	-
rename	X	X	-	-
chmod	X	-	X	X
chown	X	-	-	-
create	X	-	X	X
mkdir	X	-	-	-
rmdir	X	-	-	-
chdir	X	-	-	-

Hinweis 2

Der Wert der Abschnitte *Dateiberechtigungen* und *neue Berechtigungen* entspricht der Access Control List (acl). Diese Abschnitte können nur die Werte „SUID“ oder „SGID“ haben.

Hinweis 3

Die Direktive *Unixfile:link* hat eine andere Bedeutung, wenn sie mit Abschnitt *files* und Abschnitt *source* kombiniert wird:

- In Kombination mit dem Abschnitt *files* bedeutet sie, dass das Erstellen eines Links zur Datei im Abschnitt *files* überwacht wird.
- In Kombination mit Abschnitt *source* bedeutet dies, dass kein Link mit dem Namen erstellt werden kann, der im Abschnitt *source* angegeben wurde.

Hinweis 4

Die Richtlinie *Unixfile:rename* hat eine andere Bedeutung, wenn sie mit Abschnitt *files* und Abschnitt *source* kombiniert wird:

- In Kombination mit dem Abschnitt *files* bedeutet sie, dass die Umbenennung der Datei im Abschnitt **files** überwacht wird.
- In Kombination mit dem Abschnitt *source* bedeutet sie, dass keine Datei in die Datei im Abschnitt *source* umbenannt werden kann.

Erweiterte Details

Einige oder alle der folgenden Parameter werden in der Registerkarte „Erweiterte Details“ von Sicherheitsereignissen für die Klasse *UNIX_Files* angezeigt. Die Werte dieser Parameter können verdeutlichen, weshalb eine Signatur ausgelöst wird.

Name der grafischen Benutzeroberfläche	Erklärung
files	Die Namen der Datei, auf die zugegriffen wurde oder auf die versucht wurde, zuzugreifen.
source	Trifft nur zu, wenn die Operation die Erstellung eines symbolischen Links zwischen Dateien ist: Name des neuen Links; oder wenn die Operation die Umbenennung einer Datei ist: neuer Name der Datei.
file permission	Berechtigungen der Datei.
source permission	Trifft nur zu, wenn die Operation die Erstellung eines symbolischen Links zwischen Dateien ist: Berechtigungen für die Zieldatei (die Datei, auf die der Link verweist).
new permission	Trifft nur zu, wenn eine neue Datei erstellt oder wenn eine chmod-Operation durchgeführt wird: Berechtigungen für die neue Datei.

Klasse UNIX_apache

In der folgenden Tabelle sind die möglichen Abschnitte der Klasse *Unix_apache* aufgeführt. Diese Klasse kann für Apache-, iPlanet- und Netscape Enterprise-Webserver verwendet werden.

Abschnitt	Werte	Bedeutung/Anmerkungen
Class	UNIX_apache	
Id	4000 – 7999	
level	0, 1, 2, 3, 4	
time	*	
user_name	Benutzer- oder Systemkonto	
application	Pfad- und Anwendungsname	
url		Dieser Abschnitt ist optional. Dieser Abschnitt wird mit dem „URL“-Teil einer eingehenden Anforderung abgeglichen, siehe Hinweise 1, 2, 3, 4.
query		Dieser Abschnitt ist optional. Dieser Abschnitt wird mit dem „query“-Teil einer eingehenden Anforderung abgeglichen, siehe Hinweise 1, 2, 3, 4.
method	„GET“, „POST“, „INDEX“ und die anderen HTTP-Methoden	Dieser Abschnitt ist optional. Siehe Hinweis 4.
directives -c -d	apache:request	

Hinweis 1

Eine eingehende HTTP-Anforderung kann dargestellt werden als: `http://www.myserver.com/ {url}?{query}`. In diesem Dokument verstehen wir unter {url} den „URL“-Teil der HTTP-Anforderung und {query} als den „Query“-Teil der HTTP-Anforderung. Mit dieser Namenskonvention können wir sagen, dass der Abschnitt „url“ abgeglichen wird mit {url} und der Abschnitt „query“ abgeglichen wird mit {query}.

Beispielsweise würde die folgende Regel ausgelöst, wenn die HTTP-Anfrage `http://www.eigenerserver.de/search/abc.exe?subject=wildlife&environment=ocean` durch IIS empfangen würde:

```
Rule {
   Klasse UNIX_apache
   Id 4001
   level 1
   url { Include „*abc*“ }
   time { Include „*“ }
   application { Include „*“}
   user_name { Include „*“ }
   directives -c -d apache:request
   }
```

Diese Regel wird ausgelöst, weil {url}=/search/abc.exe, wodurch der Wert des Abschnitts „url“ abgeglichen wird (d. h. abc).

Hinweis 2

Bevor der Abgleich durchgeführt wird, werden die Abschnitte „url“ und „query“ dekodiert und normalisiert, sodass Anforderungen nicht mit Kodierungs- oder Escape-Sequenzen gefüllt werden können.

Hinweis 3

Eine Beschränkung für die maximale Länge kann für die Abschnitte „url“ und „query“ festgelegt werden. Durch Hinzufügen von „`;number-of-chars`“ zum Wert dieser Abschnitte kann diese Regel nur abgeglichen werden, wenn {url} oder {query} aus mehr Zeichen besteht als „number-of-chars“. Für die folgende Regel wird z. B. eine Übereinstimmung gefunden, wenn der URL-Teil der Anforderung „abc“ enthält und mehr als 500 Zeichen umfasst:

```
Rule {
   Klasse UNIX_apache
   Id 4001
   level 1
   url { Include „*abc*;500“ }
   time { Include „*“ }
   application { Include „*“}
   user_name { Include „*“ }
   directives -c -d apache:request}
   }
```

Hinweis 4

Eine Regel muss mindestens eine der optionalen Abschnitte „url“, „query“ und „method“ enthalten.

Benutzerdefinierte Linux-Signaturen

Dieses Thema beschreibt, wie benutzerdefinierte Linux-Signaturen geschrieben werden.

Die Klasse der Signatur hängt von der Natur des Sicherheitsproblems ab und vom Schutz, den die Regeln bieten können. Die Tabelle unten zeigt die verfügbaren Linux-Klassen:

Klasse	Bedeutung/Anmerkungen
UNIX_file	Verwendet für Datei- oder Verzeichnisoperationen. Siehe *Klasse UNIX_file*.

Klasse UNIX_file

In der folgenden Tabelle sind die möglichen Abschnitte der Klasse *Files* aufgeführt.

Abschnitt	Werte	Bedeutung/Anmerkungen
Class	UNIX_file	
Id	4000 – 7999	
level	0, 1, 2, 3, 4	
time	*	
user_name	Benutzer- oder Systemkonto	
application	Benutzer- oder Systemkontopfad + Anwendungsname	
Dateien	Quelldatei(en)	Zu suchende Dateien. Dies ist optional, wenn die Abschnittsquelle verwendet wird; siehe Hinweis 1.
Richtlinien	unixfile:link	Erstellen von Hard-Links.
	unixfile:read	Öffnen der Datei im Lesemodus.
	unixfile:write	Öffnen der Datei im Schreibmodus.
	unixfile:unlink	Löschen einer Datei aus einem Verzeichnis oder Löschen des Verzeichnisses.
	unixfile:rename	Umbenennen der Datei.
	unixfile:setattr	Ändern der Berechtigungen und der Dateieigentümerschaft des Verzeichnisses oder der Datei.
	unixfile:create	Erstellen einer Datei.
	unixfile:mkdir	Erstellen eines Verzeichnisses.
	unixfile:rmdir	Entfernen eines Verzeichnisses.

Zusammenfassung der Parameter und Richtlinien

Im Folgenden finden Sie eine Zusammenfassung der Parameter und Richtlinien entsprechend dem Typ.

Liste der Parameter entsprechend dem Typ

Typ	Parameter
Dateien, Windows-Plattform	Anwendung, Zieldatei, Dateien, Benutzername
HTTP, Windows-Plattform	Anwendung, Methode, Anforderung, URL, Benutzername
Dateien, Solaris- und Linux-Plattform	Anwendung, Quelle, Dateien, Benutzername
Registrierung	Anwendung, Registrierungsschlüssel, Benutzername, Registrierungswert
Dienste	Anwendung, Anzeigename, Dienst, Benutzername
Apache-, Solaris-Plattform	Anwendung, URL, Anforderung, Methode, Benutzername

Liste der Richtlinien entsprechend dem Typ

Typ	Richtlinien
Dateien, Windows-Plattform	create, read, write, execute, delete, rename, attribute
HTTP, Windows-Plattform	request
Dateien, Solaris-Plattform	create, symlink, link, chown, chmod, write, rmdir, chdir, read, unlink, mkdir, rename
Dateien, Linux-Plattform	create, link, setattr, write, rmdir, read, unlink, mkdir, rename
Registrierung	create, read, delete, modify, permissions, enumerate, monitor, restore, replace, load
Dienste	start, stop, pause, continue, startup, profile_enable, profile_disable, logon, create, delete
Apache-, Solaris-Plattform	request

Glossar

Adaptiver Modus
Die Schutzeinstellung für einen HIP-Client, in der die Regeln automatisch erlernt und hinzugefügt werden, ohne dass der Benutzer eingreifen muss. Dieser Modus gilt für IPS, Firewall und Anwendungsblockierregeln.

Agent-Aktivierungsaufruf
Die Möglichkeit, eine Kommunikation zwischen Agent und Server von der Serverseite aus zu initiieren.

Siehe auch *SuperAgent-Aktivierungsaufruf*.

Agenten-Host
Siehe *Client-Computer*.

Aggregierte Ansicht
Eine Ansicht von identischen Elementen, die in einer einzelnen Einheit gruppiert sind.

Aktualisieren
Das Installieren von Aktualisierungen für vorhandene Produkte oder das Aktualisieren von neuen Produktversionen.

Aktualisierungspaket
Paketdateien von McAfee, die Aktualisierungen für ein Produkt zur Verfügung stellen. Alle Pakete werden als Produktaktualisierungen betrachtet, mit der Ausnahme der Binärdateien (Setup) des Produkts.

Alternativ-Repository
Ein Typ von Repository für verteilte Software, die verwendet wird, wenn Client-Computer keines der vordefinierten verteilten Repositories kontaktieren können. In der Regel handelt es sich um ein anderes Ursprungs-Repository, das als Alternativ-Repository definiert ist.

Siehe auch *Replizieren, Replikation*.

Angriff
Eine versuchte Verletzung der Systemsicherheit. Angriffe sind eingeteilt in Stufen von „Niedrig“ (jemand hat unberechtigten Einblick in die Daten auf dem System) bis „Hoch“ (jemand zerstört oder stiehlt Daten oder bringt das System zum Stillstand).

Angriff
Eine versuchte Verletzung der Systemsicherheit. Angriffe sind eingeteilt in Stufen von „Niedrig“ (jemand hat unberechtigten Einblick in die Daten auf dem System) bis „Hoch“ (jemand zerstört oder stiehlt Daten oder bringt das System zum Stillstand).

Anwendung mit hohem Risiko
Eine Anwendung unter Anwendungsschutzregeln, in die Code in den Speicherplatz oder in die dynamische Bibliothek eingefügt werden kann, und die deshalb Schutz benötigt.

Anwendungsblockierung
Eine Funktion, die bestimmte Anwendungen gestattet oder blockiert. Es sind zwei Arten von Anwendungsblockierung verfügbar: Anwendungserstellung und Anwendungs-Hooks.

ASCI
Siehe *Kommunikationsintervall zwischen Agent und Server.*

Ausnahmeregel
Eine Regel, die eine legitime Aktivität gestattet, die andernfalls durch eine Signatur blockiert würde.

Automatische Installation
Eine Installationsmethode, bei der ein Software-Paket automatisch auf einem Computer installiert wird, ohne dass eine Benutzerintervention erforderlich ist.

Back Orifice
Ein Tool zur Remote-Verwaltung, das einen unerwünschten Zugriff auf und die Kontrolle eines Computers durch seine Internetverbindung ermöglichen kann. Es kann unter Windows 95, Windows 98 und Windows NT ausgeführt werden.

Backdoor
Eine geplante Sicherheitsverletzung in einer Anwendung, die einen unberechtigten Zugriff auf Daten gestatten kann.

Benutzerdefiniertes Agenteninstallationspaket
Ein Agenteninstallationspaket, das die Benutzerberechtigungen verwendet, die Sie zum Durchführen der Installation angeben anstelle der Benutzerberechtigungen des gegenwärtig angemeldeten Benutzers.

Bereitstellen, Bereitstellung
Die Verteilung, Installation und Konfiguration von Client-Computern von einem zentralen Ort aus.

Blockierter Host
Ein bestimmter Host, von dem es Host Intrusion Prevention erlaubt, die Kommunikation zu blockieren; sie versucht, den Ursprung des Pakets zu ermitteln, das vom blockierten Host empfangen wurde.

Brute-Force
Eine Hacker-Methode zum Herausfinden von Kennwörtern oder Verschlüsselungsschlüsseln, indem jede mögliche Kombination von Zeichen ausprobiert wird, bis der Code „geknackt" ist.

Camping Out
Eine Hacker-Technik, mit der in das System eingedrungen und anschließend ein sicherer Platz gesucht wird, von dem aus das System überwacht werden kann und Daten gespeichert werden können oder zum erneuten Eindringen in das System zu einem späteren Zeitpunkt.

Client-Computer
Ein Computer, auf dem der ePolicy Orchestrator-Agent und der Host Intrusion Prevention-Client installiert sind.

Client-Regeln
Eine IPS-, Firewall- oder Anwendungsblockierregel, die auf einem Client erstellt wurde, um legitime Aktivitäten zu erlauben, die sonst blockiert würden. Client-Regeln sind nicht Teil einer Serverrichtlinie, können jedoch für die Anwendung auf anderen Clients in einer Richtlinie verschoben werden.

Common Framework
Die Architektur, die es verschiedenen McAfee-Produkten gestattet, gemeinsame Komponenten und Codes zu verwenden. Dabei handelt es sich um Scheduler, AutoUpdate und ePolicy Orchestrator-Agent.

Computer
In der Konsolenstruktur werden die physischen Computer im Netzwerk durch ePolicy Orchestrator verwaltet. Computer können unter vorhandenen Sites oder Gruppen im **Verzeichnis** hinzugefügt werden.

DAT-Dateien
Virusdefinitionsdateien, auch Signaturdateien genannt.

Siehe auch *EXTRA.DAT-Datei*, *inkrementelle DAT-Dateien* und *SuperDAT.*

Denial of Service
Eine Angriffsmethode, bei der ein Computer mit Pseudoanforderungen überflutet wird, wodurch er abstürzt oder legitime Anforderungen nicht mehr bearbeiten kann.

Denial of Service-Angriff (DoS)
Ein Angriff, eine Intrusion, gegen einen Computer, Server oder ein Netzwerk, der die Reaktion auf legitime Verbindungsanforderungen unterbindet. Ein Denial of Service-Angriff überflutet sein Ziel mit falschen Verbindungsanforderungen, sodass das Ziel legitime Anforderungen ignoriert.

Detailbereich
Der rechte Bereich der ePolicy Orchestrator-Konsole, in dem Einzelheiten über das gegenwärtig ausgewählte Konsolenstrukturelement angezeigt werden.

Download-Site
Die McAfee-Website, von der Sie Produkt- oder DAT-Aktualisierungen abrufen können.

Siehe auch *Update-Site*.

effektive Richtlinie
Eine Zusammenführung aller Richtlinien für IPS-Regeln und für Regeln für vertrauenswürdige Anwendungen, die für Client-Computer gelten.

Eigenschaften
Daten, die während der Kommunikation zwischen Agent und Server ausgetauscht werden und die Informationen über jeden verwalteten Computer (z. B. Hard- und Software) und den verwalteten Produkten (z. B. bestimmte Richtlinieneinstellungen und die Produktversionsnummer) umfassen.

Einchecken
Das Hinzufügen von Dateien zum Master-Repository.

Element
Siehe *Konsolenstrukturelement*.

ePolicy Orchestrator-Agent
Ein Programm, das Hintergrundaufgaben auf verwalteten Computern durchführt, alle Anfragen zwischen dem ePolicy Orchestrator-Server und den Anti-Virus- und Sicherheitsprodukten auf diesem Computern verhandelt und wiederum dem Server berichtet, um den Status dieser Tasks anzugeben.

ePolicy Orchestrator-Datenbank
Die Datenbank, in der alle Daten, die durch ePolicy Orchestrator-Server von ePolicy Orchestrator-Agenten empfangen wurden, und alle Einstellungen gespeichert sind, die auf dem Server vorgenommen wurden.

Siehe auch *ePolicy Orchestrator-Datenbank-Server*.

ePolicy Orchestrator-Datenbank-Server
Der Computer, der als Host für die ePolicy Orchestrator-Datenbank dient. Dabei kann es sich um denselben Computer handeln, auf dem der ePolicy Orchestrator-Server installiert ist, oder um einen separaten Computer.

ePolicy Orchestrator-Konsole
Die Benutzeroberfläche der ePolicy Orchestrator-Software, die für die Remote-Steuerung und die Überwachung von verwalteten Computern verwendet wird.

Siehe auch *ePolicy Orchestrator-Remote-Konsole*.

ePolicy Orchestrator-Remote-Konsole
Die ePolicy Orchestrator-Benutzeroberfläche, wenn sie auf einem separaten Computer vom ePolicy Orchestrator-Server installiert wird.

Siehe auch *ePolicy Orchestrator-Konsole*.

ePolicy Orchestrator-Server
Die Back-End-Komponente der ePolicy Orchestrator-Software.

Siehe auch *ePolicy Orchestrator-Agent* und *ePolicy Orchestrator-Konsole*.

Ereignis
Eine Warnung, die ausgelöst wird, wenn ein Sicherheitsverstoß vorliegt, wie er durch eine Signatur definiert wurde. Alle Ereignisse, die auf einem ausgewählten Host ausgelöst werden, sind in der IPS-Liste aufgeführt.

Siehe auch *Signatur*.

Erzwingen der Installation, Erzwingen der Deinstallation
Siehe *Produktbereitstellung-Client-Task*.

Erzwingen, Erzwingung
Das Anwenden von vordefinierten Einstellungen auf Client-Computern in festgelegten Intervallen.

EXTRA.DAT-Datei
Zusätzliche Virusdefinitionsdatei, die als Reaktion auf den Ausbruch eines neuen Virus oder einer neuen Variante eines bereits vorhandenen Virus erstellt wird.

Siehe auch *DAT-Dateien*, *inkrementelle DAT-Dateien* und *SUPERDAT*.

Falsch-Positive
Ein Ereignis, das durch eine legitime Operation eines zulässigen Prozesses und nicht durch eine Intrusion ausgelöst wird.

Fehlerbericht-Dienstprogramm
Ein Dienstprogramm, das ausschließlich zum Zweck des Verfolgens und Protokollierens von Fehlern der McAfee-Software auf dem System entworfen wurde. Die erhaltenen Daten können bei der Analyse von Problemen hilfreich sein.

Firewall
Ein Filter zwischen einem Computer und Netzwerkverbindungen, der es erlaubt, Verkehr auf der Grundlage von Firewall-Regeln zu erlauben oder zu blockieren. Mit statusbehafteter Filterung wird der Status von Verbindungen nachverfolgt, und mit der statusbehafteten Inspizierung wird die Nachverfolgung von Befehlen, die im Netzwerkstapel höher liegen, überprüft, was sowohl eine stärkere Kontrolle als auch eine höhere Sicherheit der Verbindungen ermöglicht.

FRAMEPKG.EXE
Siehe *Agenteninstallationspaket*.

Funktion
Eine funktionale Division eines Produkts. Host Intrusion Prevention umfasst die Funktionen „IPS", „Firewall", „Anwendungsblockierung" und „Allgemein".

Global verteiltes Repository
Ein verteiltes Software-Repository, das automatisch auf demselben Stand wie das Master-Repository gehalten werden kann.

Siehe auch *Replizieren, Replikation*.

Globale Aktualisierung
Eine Methode für die Bereitstellung von Produktaktualisierungen ohne Benutzerintervention, sobald die Dateien in das Master-Repository eingecheckt sind. Die Dateien werden sofort in allen SuperAgent- und global verteilten Repositories repliziert; der ePolicy Orchestrator-Server sendet einen Aktivierungsaufruf an alle SuperAgents. Die SuperAgents übertragen einen Aktivierungsaufruf an alle Agenten auf demselben Subnetz, und alle Client-Computer rufen die aktualisierten Dateien aus dem nächsten Repository ab.

Globale Richtlinie
Die McAfee-Standardrichtlinie für eine Kategorie.

Globale Schwarze Liste
Eine Liste von E-Mail-Adressen oder Domänen, die der Administrator als unternehmensweiten Standard einrichtet. Alle E-Mail-Nachrichten von Adressen oder Domänen der globalen Schwarzen Liste werden stets als Spam betrachtet.

Siehe auch *Globale Weiße Liste*; siehe auch *Schwarze Liste*.

Globale/McAfee-Standardrichtlinie
Die grundlegenden Richtlinieneinstellungen für eine Kategorie, die sofortigen Schutz bieten.

Globaler Administrator
Ein Benutzerkonto mit Lese-, Schreib- und Löschberechtigungen sowie Berechtigungen für alle Operationen, insbesondere Operationen, die die gesamte Installation betreffen und die reserviert sind für die ausschließliche Verwendung durch den globalen Administrator.

Siehe auch *Globaler Prüfer*, *Site-Administrator*, *Site-Prüfer*.

Globaler Prüfer
Ein Benutzerkonto mit ausschließlicher Leseberechtigung, mit dem alle Einstellungen der Software für eine vollständige Installation angezeigt, aber nicht geändert werden können.

Siehe auch *Globaler Administrator*, *Site-Administrator*, *Site-Prüfer*.

Gruppe „Verloren & Gefunden“
Eine Gruppe, die zum temporären Speichern von Computern verwendet wird, deren richtiger Standort im **Verzeichnis** nicht bestimmt werden kann.

Gruppe
In der Konsolenstruktur handelt es sich um eine logische Sammlung von Einheiten, die für eine vereinfachte Verwaltung zusammengefasst wurden. Gruppen können andere Gruppen oder Computer enthalten; man kann ihnen IP-Adressbereiche oder IP-Subnetzmasken zuweisen, um das Sortieren von Computern nach IP-Adressen zu ermöglichen. Wenn Sie eine Gruppe durch Importieren einer Windows NT-Domäne erstellen, können Sie automatisch das Agenteninstallationspaket an alle importierten Computer in der Domäne senden.

Host Intrusion Prevention (HIP)-Client
Das Host Intrusion Prevention-Modul, das auf jedem Host-System im Netzwerk installiert ist. Ein Client dient als „Schutzschicht“ für das Betriebssystem und die Anwendungen eines Computers. Er erkennt und verhindert potentielle Sicherheitsrisiken und gefährliche Angriffe.

Host, Host-Computer
Siehe *Client-Computer*.

Host-IPS (HIPS)
Host-Schutzregeln, die Angriffe auf das Betriebssystem und auf Anwendungen auf einem Host-System überwachen und verhindern.

HotFix-Versionen (jetzt Patches)
Zwischenversionen des Produkts, die bestimmte Probleme beheben.

Inaktive Agenten
Jeder Agent, der nicht innerhalb eines festgelegten Zeitraumes mit ePolicy Orchestrator kommuniziert hat.

Kategorie
Ein Teil einer Funktion von Host Intrusion Prevention, der Sie eine Richtlinie zuweisen können. Beispielsweise umfasst die IPS-Funktion die Kategorien „IPS-Optionen“, „IPS-Schutz“ und „IPS-Regeln“.

Knoten
Siehe *Konsolenstrukturelement*.

Kommunikation zwischen Agent und Server
Jegliche Kommunikation, die zwischen ePolicy Orchestrator-Agenten und dem ePolicy Orchestrator-Server stattfindet, bei der Agenten und Server Daten austauschen. In der Regel initiiert der Agent die gesamte Kommunikation mit dem Server.

Kommunikationsintervall zwischen Agent und Server (Agent-to-Server Communication Interval, ASCI)
Der Zeitraum zwischen der vordefinierten Kommunikation zwischen Agent und Server

Konfigurationseinstellungen
Siehe *Richtlinie*.

Konsolenstruktur
Die Inhalte der Registerkarte **Struktur** im linken Bereich der ePolicy Orchestrator-Konsole. Sie zeigt die in der Konsole verfügbaren Elemente an.

Konsolenstrukturelement
Die einzelnen Symbole in der Konsolenstruktur der ePolicy Orchestrator-Konsole.

Lernmodus
Die Host Intrusion Prevention-Schutzeinstellung, in der Regeln erlernt und hinzugefügt werden, nachdem ein Benutzer auf eine Aufforderung reagiert, eine Aktion zu erlauben oder zu blockieren. Dieser Modus gilt für die Firewall- und Anwendungsblockierfunktionen.

Lokal verteiltes Repository
Ein Typ von verteiltem Software-Repository, dessen Inhalt manuell aktualisiert wird.

Master-Repository
Ein Typ von verteiltem Software-Repository, dessen Inhalte als Standard dienen für alle anderen verteilten Repositories. In der Regel sind die Inhalte des Master-Repositories als Kombination der Inhalte des Ursprungs-Repositories und zusätzlichen Dateien definiert, die manuell zum Master-Repository hinzugefügt wurden.

Siehe auch *Ziehen*; *Replizieren, Replikation*.

.NAP-Datei
Diese Dateierweiterung bezeichnet McAfee-Software-Programme, die im Software-Repository für die Verwaltung durch ePolicy Orchestrator installiert werden.

Netzwerk-IPS (NIPS)
Netzwerkschutzregeln, die Netzwerkangriffe überwachen und verhindern.

Paketkatalogdatei
Eine Datei, die Details über jedes Aktualisierungspaket, einschließlich des Namens des Produkts, enthält, für das die Aktualisierung gedacht ist, die Sprachversion und etwaige Installationsabhängigkeiten.

Ping of Death
Eine Hacker-Technik, mit deren Hilfe ein System durch Senden von großen ICMP-Paketen an ein Ziel lahm gelegt wird. Während das Ziel versucht, das Paket neu anzuordnen, führt die Paketgröße zu einem Pufferüberlauf und kann zum Neustart oder Hängen des Zieles führen.

Ping-Angriff
Das Überfluten eines Netzwerks mit `ping`-Befehlen.

Port-Scanning
Eine Hacker-Technik, mit deren Hilfe TCP/IP-Ports geprüft werden, um herauszufinden, welche Dienste verfügbar sind. Über diese Dienste wird dann die Sicherheitsverletzung geplant und das Betriebssystem eines bestimmten Computers festgestellt.

Produktbereitstellung-Client-Task
Ein geplanter Task für die Bereitstellung aller Produkte, die gerade in das Master-Repository auf einmal eingecheckt werden. Mit ihm können Sie die Produktinstallation abseits der Hauptbelastungszeiten oder während des Richtliniendurchsetzungsintervalls planen und entfernen.

Profil
Eine Gruppierung von Richtlinien, die auf häufig verwendeten Anwendungen, dem Netzwerk-Speicherort oder auf Zugriffsrechten und -berechtigungen basiert.

Pufferüberlaufangriff
Die Methode des Überfüllens eines Software-Puffers, um anderen Code mit höheren Berechtigungen einzubringen und auszuführen; häufig handelt es sich dabei um eine Shell, von der aus weitere Befehle ausgegeben werden können.

Quarantänemodus
Die erzwungene Isolation eines Computers, bis die Schutzrichtlinien aktualisiert werden können.

Reaktion
Die Antwort eines Client beim Abfangen einer Signatur. Es gibt drei mögliche Reaktionen: **Ignorieren** (ignoriert die Operation), **Protokollieren** (protokolliert die Operation in der Datenbank als Intrusion) und **Verhindern** (verhindert eine bestimmte illegale Operation und protokolliert sie).

Remote-Konsole
Siehe auch *ePolicy Orchestrator-Remote-Konsole*.

Repository
Der Speicherort für die Richtlinienseiten, die für die Produktverwaltung verwendet werden.

Richtlinie

Eine Gruppe von Einstellungen, die einer Kategorie einer Produktfunktion zugewiesen ist. Für die meisten Kategorien ist nur eine benannte Richtlinie für jede Kategorie gestattet. Ausnahmen sind IPS-Regeln und Anwendungsregeln, bei denen eine oder mehrere benannte Richtlinien angewendet werden können.

Richtliniendateien
Satz von Richtlinieneinstellungen für ein oder mehrere Produkte, die auf dem lokalen Laufwerk des ePolicy Orchestrator-Servers gespeichert werden, auf die jedoch kein Zugriff von einer Remote-Konsole möglich ist.

Siehe auch *Richtlinienvorlagen*.

Richtliniendurchsetzungsintervall
Der Zeitraum, in dem der Agent die Einstellungen durchsetzt, die er vom ePolicy Orchestrator-Server erhalten hat. Da diese Einstellungen lokal durchgesetzt werden, ist für dieses Intervall keine Bandbreite erforderlich.

Richtlinienseiten
Teil der ePolicy Orchestrator-Konsole; sie gestatten Ihnen, die Richtlinien festzulegen und geplante Tasks für Produkte zu erstellen. Sie werden auf einzelnen ePolicy Orchestrator-Servern gespeichert (sie werden nicht zum Master-Repository hinzugefügt).

Selektive Aktualisierung
Die Möglichkeit festzulegen, welche Aktualisierungsversion von Client-Computern aus verteilten Software-Repositories abgerufen werden soll.

Siehe auch *Verzweigung*.

Server-Tasks
Tasks, die auf der Server-Seite der Software ausgeführt werden können.

Signatur
Der Satz von Regeln, der Sicherheitsbedrohungen und Anweisungen für einen Host oder ein Netzwerk beschreibt. Jeder dieser drei Typen von IPS-Signaturen, Host (HIPS), Benutzerdefiniert (HIPS) und Netzwerk (NIPS), hat eine zugeordnete Sicherheitsebene, die die Gefahr des potentiellen Angriffs angibt.

Siehe auch *Verhaltensregel*.

Signaturdateien
Siehe *DAT-Dateien*.

Sicherheitsebene
Eine von vier Risikoebenen, die Signaturen zugewiesen werden können:

Informationen (blau) – eine Änderung an der Systemkonfiguration oder ein Versuch, auf sensitive Systemkomponenten zuzugreifen, die jedoch nicht grundsätzlich ein Nachweis für einen Angriff sind.

Niedrig (gelb) – eine Änderung an der Systemkonfiguration oder ein Versuch, auf sensitive Systemkomponenten zuzugreifen, die jedoch nicht als bekannte Angriffe erkannt werden und auf ein verdächtiges Verhalten eines Benutzers oder einer Anwendung hinweisen.

Mittel (orange) – ein bekannter Angriff mit mittlerem Risiko oder ein hochverdächtiges Verhalten durch einen Benutzer oder eine Anwendung.

Hoch (rot) – Angriff, der eine ernsthafte Bedrohung für die Sicherheit darstellt.

Site-Administrator
Ein Benutzerkonto mit Lese-, Schreib- und Löschberechtigungen sowie Berechtigungen für alle Operationen für die angegebene Site (mit Ausnahme von solchen, die nur für den globalen Administrator freigegeben sind) und für alle Gruppen und Computer, die untergeordnete Elemente in der Konsolenstruktur sind.

Siehe auch *Globaler Prüfer*, *Globaler Administrator*, *Site-Prüfer*.

Site
In der Konsolenstruktur handelt es sich um eine logische Sammlung von Einheiten, die für eine vereinfachte Verwaltung zusammengefasst wurden. Sites können Gruppen oder Computer enthalten und nach IP-Adressbereich, IP-Subnetzmaske, Standort, Abteilung usw. angeordnet werden.

Site-Prüfer
Ein Benutzerkonto mit ausschließlicher Leseberechtigung, mit dem alle Einstellungen der Software für die festgelegte Site angezeigt, aber nicht geändert werden können.

Siehe auch *Globaler Administrator*, *Globaler Prüfer*, *Site-Administrator*.

Smurf-Angriff
Ein Denial of Service-Angriff, der sein Ziel mit Antworten auf das ICMP-Echo (`ping`) überflutet. Bei einem Smurf-Angriff werden `ping`-Anforderungen an Internet-Broadcast-Adressen gesendet, die `ping`-Anforderungen an bis zu 255 Hosts auf einem Subnetz weiterleiten. Die Rückgabeadresse der `ping`-Anforderung wird auf die Adresse des Angriffsziels gefälscht („spoofed"). Alle Hosts, die `ping`-Anforderungen empfangen, antworten auf das Angriffsziel und überfluten dabei das Ziel mit Antworten.

Snooping
Das passive Beobachten eines Netzwerks.

Spoofing
Das Fälschen von z. B. einer IP-Adresse, um den eigenen Standort und die Identität zu verbergen.

Status Monitor
Siehe *Agent Monitor*.

Status
Beschreibt die tatsächliche Funktionsweise eines Client (aktueller Status) oder die Funktion nach der nächsten Kommunikation mit dem Server (angeforderter Status). Die Konsole erkennt vier unterschiedliche Stati: **Normal**, **Deinstallation**, **Keine Verbindung**, **Keine Lizenz**.

SYN-Überflutung
Eine Hacker-Technik, die verwendet wird, um einen Denial of Service zu bewirken. SYN-Pakete werden von einem Client mit einer Spoof-IP-Adresse gesendet, mit einer höheren Geschwindigkeit als der TCP-Stapel auf dem Host bearbeiten kann. Da ein Spoofing der Client-Adresse durchgeführt wurde, sendet der Client kein SYN-ACK, sondern überflutet den Host mit SYN-Paketen und bindet dabei die Ressourcen des Hosts.

Task
Siehe *Client-Tasks*, *Server-Tasks*.

Trojaner
Ein Programm, das entweder vorgibt, eine Reihe nützlicher oder wünschenswerter Funktionen zu besitzen oder so beschrieben wird, tatsächlich aber schädliche Auswirkungen mit sich bringt. Trojaner sind technisch gesehen keine Viren, da sie sich nicht replizieren.

Tunen
Der Vorgang des Erkennens von einigen Profilen und des Erstellens von Richtlinien dafür, um die Zahl von falschen Positiven zu verringern und das Generieren von Ereignissen zu verhindern.

Übernehmen
Das Anwenden der für ein Element festgelegten Einstellungen innerhalb einer Hierarchie vom übergeordneten Element.

Verhaltensregel
Eine IPS-Regel, die ein Profil legitimer Aktivitäten definiert. Eine Aktivität, die nicht dem Profil entspricht, löst das Ereignis aus.

Siehe auch *Signatur*.

Verteilte Software-Repositories
Eine Sammlung von Websites oder Computern, die so über das Netzwerk verteilt sind, dass ein bandbreiteneffizienter Zugang zu den Client-Computern möglich ist. In verteilten Software-Repositories werden Dateien gespeichert, die Client-Computer für die Installation von unterstützten Produkten und Aktualisierungen für diese Produkte benötigen.

Siehe auch *Alternativ-Repository*, *Global verteiltes Repository*, *Lokal verteiltes Repository*, *Master-Repository*, *Spiegelung des verteilten Repositorys*, *Ursprungs-Repository* und *Verteiltes SuperAgent-Repository*.

Vertrauenswürdige Anwendung
Eine Anwendung, die als sicher in einer Umgebung bekannt ist, keine bekannten Schwachstellen aufweist und jede Operation durchführen darf.

Verwaltete Produkte
Ein Sicherheitsprodukt, wie Host Intrusion Prevention, das durch ePolicy Orchestrator verwaltet wird.

Verzeichnis
Die Liste aller über ePolicy Orchestrator zu verwaltenden Computer; die Verknüpfung zu den primären Benutzeroberflächen für die Verwaltung dieser Computer.

Verzweigung
Speicherorte im Master-Repository, mit deren Hilfe Sie verschiedene Versionen von ausgewählten Aktualisierungen speichern und verteilen können.

Siehe auch *Selektive Aktualisierung*.

Vollständige Eigenschaften
Alle Eigenschaften, die während einer Kommunikation zwischen Agent und Server ausgetauscht werden können.

Siehe auch *Minimale Eigenschaften*.

Vollständige Eigenschaften
Der vollständige Satz von Eigenschaften, die während der Kommunikation zwischen Agent und Server ausgetauscht werden.

Siehe auch *Inkrementelle Eigenschaften*.

Warnung
Siehe auch *Ereignis*.

Zero-Day-Angriff
Ein Programm, das Sicherheitslücken genau an dem Tag nutzt, an dem diese Lücke allgemein bekannt wird.

Ziehen
Das Kopieren von Dateien aus einem Ursprungs- oder Alternativ-Repository in das Master-Repository. Da zusätzliche Dateien zum Master-Repository manuell hinzugefügt werden können, werden nur die Dateien im Ursprungs- oder Alternativ-Repository überschrieben.

Index

A

Adaptiver Modus, 23, 31
- Anwendungsblockierung, 31, 103
- Firewall, 31, 81
- IPS, 31, 39

Aktualisieren
- Clients, 140
- Einchecken des Updates, 139
- Inhalt, 139
- Prozess, 139

Anwendungsblockierregeln, 106
- Erstellen, 107
- Löschen, 108

Anwendungsblockierung
- Client-Regeln, 19
- Direktzugriff, 102
- erstellen, 101
- Hooking, 102
- Konfigurieren der Optionen, 103
- Überblick, 101
- vordefinierte Richtlinien, 102

Anwendungsblockierungs-Client-Regeln
- Aggregierte Ansicht, 109
- Anzeigen, 109
- Standard-Ansicht, 109

Anwendungsschutzregeln, 56
- Aktivieren, 60
- Bearbeiten, 60
- Deaktivieren, 60
- Erstellen, 58
- Löschen, 60
- Überblick, 56

Ausnahmeregeln, 17
- Aktivieren, 48
- Bearbeiten, 47
- Deaktivieren, 48
- Erstellen, 46
- Erstellung basierend auf einem Ereignis, 66
- Löschen, 48
- suchen, 70
- Suchen nach verknüpften, 67
- verschieben in eine andere Richtlinie, 48, 70

Avert Labs – Bedrohungsbibliothek, 14

Avert Labs – Bedrohungszentrum, 14

B

Bedrohungsbibliothek, 14

Bedrohungszentrum (*Siehe* Avert Labs)

Benachrichtigungen
- generieren, 29
- Typen, 133
- Verwendung, 132

benutzerdefiniert
- Hostsignaturen, 49
- Signaturen, weitere Informationen, 55

Bereitstellung
- Feineinstellung, 124
- Tunen, 23, 33, 124, 175

Berichte, 24
- auflisten, 135
- ausführen, 134
- Fehlgeschlagene Quarantäne-Updates, 139
- generieren, 29
- IPS-Ereigniszusammenfassung nach Signatur, 136
- IPS-Ereigniszusammenfassung nach Ziel, 136
- Netzwerk-Intrusionszusammenfassung nach Quell-IP, 137
- Top 10 der angegriffenen Knoten für IPS, 137
- Top 10 der aufgerufenen Signaturen, 138
- Top 10 der blockierten Anwendungen, 138
- vordefiniert, 134
- Zusammenfassung der blockierten Anwendungen, 138

Bewerten von McAfee-Produkten, Download-Website, 14

C

Client-Regeln
- Anwendungsblockierung, 109
- Firewall, 18, 94
- IPS, 68

D

DAT-Dateien
- Avert Labs-Benachrichtigungsdienst für Aktualisierungen, 14
- Updates, Website, 14

Definition von Begriffen (*siehe* Glossar)

Direktzugriff
- Anwendungsblockierregeln, 102
- Anwendungsblockierungs-Client-Regeln, 102
- Firewall-Client-Regeln, 84
- Firewall-Regeln, 84
- IPS-Client-Regeln, 39
- IPS-Ereignisse, 39
- IPS-Regeln, 39

Download-Website, 14

E

Einsenden eines Beispiels, Avert Labs WebImmune, 14

ePO
- Benachrichtigungen, 29
- Berichte, 29
- Konsole, 26
- mit Host Intrusion Prevention verwendete Vorgänge, 26
- Richtlinieneigentümer, 28
- Richtlinienverwaltung, 27

Erzwingen von Richtlinien
- Linux-Client, 167

Erzwingen von Richtlinien
- Solaris-Client, 164

F

Firewall
- Adaptiver Modus, 81
- Funktionsübersicht, 73
- Lernmodus, 81

Migration in statusbehaftete Regeln, 83
Paketfilterung, 74
Paketinspizierung, 74
Quarantäneregeln, 82
Quarantäneregeln, Richtlinie, 97
Regelgruppen, 79
Regeln, 17
Statustabelle, 74
Verbindungsgruppen, 79
Verbindungsregeln, 79
vordefinierte Richtlinien, 84
Firewall-Client-Regeln
aggregieren, 95
Aggregierte Ansicht, 95
Anzeigen, 94
Direktzugriff, 84
Standard-Ansicht, 94
Firewall-Regelgruppe
Erstellen, 91
Löschen, 94
Firewall-Regeln, 76
6.0, 73
6.1, 74
Anzeigen, 90
Bearbeiten, 90
Client, 18
Direktzugriff, 84
Erstellen, 91
Funktionsweise, 75
Hinzufügen, 91
Löschen, 94
Migration in statusbehaftete, 83
Reihenfolge, 76
statisch, 73
statusbehaftet, 74
statusbehaftete Filterung, 76
statusbehaftete Inspizierung, 77
Statusbehaftete Protokollverfolgung, 78
Firewall-Regeln, Richtlinie
Erstellen, 87
Konfigurieren, 87
vordefinierte Richtlinien, 87
Funktion „Allgemein“
Überblick, 111
vordefinierte Richtlinien, 112
Funktionen
Allgemein, 19
Anwendungs-blockierung, 18, 101
Firewall, 17, 73
IPS, 15, 36
Funktionen, neue, 10

G

Glossar, 202 to 211

H

Handbücher
Produktdokumentation, 13
Handbuchkonventionen
Schriftarten und Symbole, 12
Hilfe
Erläuterung der Symbole, 35
in der UI, 35
Verwenden, 34
Vorgehensweisen für die Navigation, 34
Host Intrusion Prevention
Arbeiten mit Clients, 30
Bereitstellen von Clients, 30
Bereitstellung, 22
Hilfe, 34
Installieren, 29
Konfigurieren, 25
Tunen, 33
Verwenden von ePO, 25 to 26
Wartung, 22
Hostsignaturen, 49
HotFixes und Patches (für Produkte und Sicherheitsschwachstellen), 14

I

Informationsbibliothek (*Siehe* Avert Labs – Bedrohungsbibliothek)
IPS
Ausnahmeregeln, 17
Client-Ausnahmeregeln, 18
Ereignisse, 16
Ereignisse, analysieren, 124
Funktion, 15
Funktionsübersicht, 36
Reaktionen, 16
Signaturen, 15
IPS-Client-Regeln, 68
aggregieren, 69
Aggregierte Ansicht, 69
migrieren in eine Richtlinie, 68
Standard-Ansicht, 68
Überblick, 68
IPS-Ereignisse, 60
ähnliche markieren, 64
als gelesen markieren., 63
als ungelesen markieren, 63
analysieren, 124
Anzeigen, 61, 174
Details, 65
Ausnahme erstellen, 66, 175
Erstellen vertrauenswürdiger Anwendungen, 66
Filtern der Ansicht, 62
Konfigurieren der Ansicht, 62
Markieren, 63
Überblick, 60
verbergen, 63
verborgene Anzeigen, 63

K

Kennwörter
Administrator, 116
für die Client-UI, 115
zeitbasiert, 117
KnowledgeBase-Zugang, 14
Kundendienst, Kontakt, 14

L

Lernmodus, 23, 31
Anwendungsblockierung, 31, 150
Firewall, 31, 81
Linux-Client
Erzwingen von Richtlinien, 167
Hinweise, 168
Problembehandlung, 168
Überblick, 167

N

Netzwerksignaturen, 49

P

Paketfilterung, 74
Paketinspizierung, Firewall, 74
Problembehandlung
Linux-Client, 168
Solaris-Client, 164
Produktaktualisierungen, 14
Produktinformationen
Ressourcen, 13
professionelle Dienstleistungen, McAfee-Ressourcen, 14

Q

Quarantäne
Richtlinien und Regeln, 82
Quarantänegruppen
Löschen, 100
Quarantäneoptionen, Richtlinie
Konfigurieren, 96
Quarantäneregelgruppen
Erstellen, 99

Quarantäneregeln
Anzeigen, 99
Bearbeiten, 99
Erstellen, 99
Hinzufügen, 99
Löschen, 100
Quarantäneregeln, Richtlinie
Erstellen, 97
Konfigurieren, 97

R

Regelgruppen
Firewall, 79
Richtlinie „Anwendungsblockierregeln“
Erstellen, 105, 107
Konfigurieren, 105
Richtlinie „Client-UI“
anwenden, 114
Erstellen, 114
Kennwörter, 115
Konfigurieren, 113
Richtlinie „IPS-Optionen“
Erstellen, 40
Konfigurieren, 39
vordefinierte Richtlinien, 39
Richtlinie „IPS-Regeln“
Anwendungsschutzregeln, 56
Ausnahmeregeln, 45
Details, 45
Erstellen, 44
Konfigurieren, 44
Signaturen, 48
zuweisen, 44
Richtlinie „IPS-Schutz“
vordefinierte Richtlinien, 42
Richtlinie „Richtlinien erzwingen“
Konfigurieren, 113
Richtlinie „Vertrauenswürdige Anwendungen“
anwenden, 120
Erstellen, 120
Konfigurieren, 120
Richtlinie „Vertrauenswürdige Netzwerke“, 118
Konfigurieren, 118
Richtlinie für Firewall-Optionen
Konfigurieren, 85
vordefinierte Richtlinien, 85
Richtlinien
Anzeigen des Eigentümers, 129
Anzeigen von Informationen, 128
Aufgaben, 126
Bearbeiten der Informationen, 129
Durchsetzung, 19, 173
Durchsetzung deaktiviert, 129
Eigentümerschaft, 21
Kategorien, 20
Konfigurieren, 32
Übereinstimmung mit einem Profil, 176
Vererbung, 21, 126
Verwalter, 173
Verwaltung, 19, 27
Verwenden der Registerkarte „Richtlinien“, 126
Verwenden des Richtlinienkatalogs, 128
vordefinierter Schutz, 22
Wartung, 126
welcher Knoten ist zugewiesen, 129
Zuweisen von Eigentümern, 28
Zuweisung, 21, 126, 173
Zuweisungssperre, 21
Richtlinien für Anwendungsblockieroptionen
Konfigurieren, 103

S

Schulung, McAfee-Ressourcen, 14
Server-Tasks, 131
Eigenschaften-übersetzung, 131
Ereignisarchivierung, 131
Verzeichnis-Gateway, 131
ServicePortal, Technischer Support, 14
Sicherheitsebenen
Hoch (Rot), 48
Information (blau), 48
Mittel (Orange), 48
Niedrig (gelb), 48
Sicherheitsschwachstellen, Veröffentlichungen für, 14
Sicherheits-Updates, DAT-Dateien und Modul, 14
Sicherheitszentrale (*Siehe* Avert Labs)
Signaturen, 48
Bearbeiten, 51
Bearbeiten benutzerdefinierter, 55
Bearbeitungsansicht, 50
benutzerdefiniert, 49, 51
Benutzerdefinierter Host, 49
Erstellen, 51
Erstellen benutzerdefiniert, 175
Erstellen im Standardmodus, 53
Erstellen mit dem Assistenten, 51
Erstellen mit dem Expertenverfahren, 55
Erstellen mit dem Standardverfahren, 55
Host, 49
Host-IPS, 37
Netzwerk, 49
Netzwerk-IPS, 37
Schweregrade, 48
Typen, 49
Solaris-Client
Erzwingen von Richtlinien, 164
Problembehandlung, 164
Überblick, 164
statusbehaftete Filterung, 76
Statusbehaftete Paketinspizierung, 77
Statusbehaftete Protokollverfolgung, 78
DHCP, 79
DNS, 78
FTP, 79
ICMP, 78
TCP, 78
Statustabelle, Firewall, 74

T

Technischer Support, kontaktieren, 14
Tunen
Analysieren von Ereignissen, 124
Anwenden neuer Richtlinien, 125
Ausnahme erstellen, 125
automatisch, 175
Client-Regeln, 125
Erstellen neuer Richtlinien, 125
Erstellen vertrauenswürdiger Anwendungen, 125

U

UDP, 78
Upgrade-Website, 14

V

Verbindungsgruppe
Erstellen, 91
Verhaltensregeln, 38

vertrauenswürdige Anwendungen
Aktivieren, 123
Bearbeiten, 123
Deaktivieren, 123
Erstellen, 121
Erstellung basierend auf einem Ereignis, 66
Löschen, 123
Vertrauenswürdige Netzwerke
Optionen, 118
Verwenden dieses Handbuchs, 11
vordefinierte Richtlinien
Allgemein, 112
Anwendungsblockierung, 102
Firewall, 84
Firewall-Optionen, 85
Firewall-Regeln, 87
IPS, 38
IPS-Optionen, 39
IPS-Schutz, 42

W

Warnungen
Active X, 32
Anwendungsblockierung, 150
Anzeigen von Richtlinien, 32
Firewall, 149
Intrusion, 148
Java-Applet, 32
Quarantäne, 151
Spoofing erkannt, 151
WebImmune, Avert Labs – Bedrohungszentrum, 14
Website für das Beta-Programm, 14
Windows-Client
Entsperren der Benutzeroberfläche, 144
Fehlerbehebung, IPS-Module, 147
Fehlerbehebung, Protokollierung, 146
Fehlerbericht, 145
Festlegen von Optionen, 145
Konsole, 144
Liste „Blockierte Hosts“, 159
Liste auf der Registerkarte „Aktivitätsprotokoll“, 163
Liste auf der Registerkarte „Anwendungsschutz“, 161
Liste der Regeln auf der Registerkarte „Anwendungsrichtlinie“, 158
Liste der Regeln auf der Registerkarte „Firewall-Richtlinie“, 156
Optionen auf der Registerkarte „Aktivitätsprotokoll“, 162
Optionen auf der Registerkarte „Anwendungsrichtlinie“, 157
Optionen auf der Registerkarte „Firewall-Richtlinie“, 155
Optionen auf der Registerkarte für IPS-Richtlinien, 153
Problembehandlung, 146
Regeln auf der Registerkarte „Anwendungsrichtlinie“, 158
Regeln auf der Registerkarte „Firewall-Richtlinie“, 156
Regeln auf der Registerkarte „IPS-Richtlinie“, 154
Regeln auf der Registerkarte „IPS-Richtlinie“, 154
Registerkarte „Aktivitätsprotokoll“, 162
Registerkarte „Anwendungsrichtlinie“, 157
Registerkarte „Anwendungsschutz“, 161
Registerkarte „Blockierte Hosts“, 159
Registerkarte „Firewall-Richtlinie“, 155
Registerkarte „IPS-Richtlinie“, 153
Systemablagensymbol, 117, 143
Überblick, 142
Warnungen, 147
Windows-Client-UI-Steuerung
Taskleistensymbol, 117
Windows-Client-Warnungen
Anwendungsblockierung, 150
Firewall, 149
Intrusion, 148
Quarantäne, 151
Spoofing erkannt, 151

Z

Zielgruppe fdes Handbuchs, 11

700-1499-15

Copyright © 2006 McAfee, Inc. Alle Rechte vorbehalten.

McAfee®

mcafee.com